Budapesti Műszaki és Gazdaságtudományi Egyetem
Villamosmérnöki és Informatikai Kar
Hálózati Rendszerek és Szolgáltatások Tanszék

Mihály András

Megbízható földi és műholdas csomópontokon alapuló kvantumkulcsszétosztó rendszer vizsgálata

KONZULENS
Dr. Bacsárdi László

BUDAPEST, 2020

Tartalomjegyzék

Összefoglaló

A mai világ biztonságos kommunikációjának nagy része azon alapul, hogy a nyilvános kulcsú titkosítást csak nagyon lassan lehet feltörni. Bár tény, hogy a ma létező legerősebb klasszikus számítógépeknek is beláthatatlanul sok időbe telne feltörni az RSA-n alapuló titkosítást, ez nem feltétlenül igaz más nem konvencionális rendszerekre, mint például a kvantumszámítógépekre. Peter Shor kvantumalgoritmusának köszönhetően tudjuk, hogy el fog érkezni az idő, amikor a nyilvános kulcsú titkosítás feltörése nem évezredek, hanem másodpercek kérdése lesz.

Ugyanakkor, a szimmetrikus kulcson alapuló titkosítás a kvantumszámítógépek korában is megfelelő biztonságot fog nyújtani. A kérdés csupán az, hogyan osztjuk meg a titkosításhoz használt szimmetrikus kulcsot a kommunikáló felek között. Ezt a műveletet végrehajthatjuk kvantumkulcsszétosztással. Bár ez egy egyszerű és jól bevált módszer, de alapvetően pont-pont között működik. A kvantumkulcsszétosztó rendszerek hálózatba kötésével viszont már új irányok nyílnak meg és kvantuminternetről tudunk beszélni. Olyan rendszerekről, amelyek kvantumkulcsszétosztáson túlmenően kvantumos információk szállítására is alkalmasak, vezetékes, illetve szabadtéri linkek felhasználásával.

Munkám során kvantumkommunikációs rendszerek szimulációjával foglalkoztam. Egy, két földi pontot műholdrendszerrel összekötő kvantumkommunikációs-rendszer szimulációját készítettem el. Ebben annak a lehetőségét vizsgáltam, hogy az eddig sokszor használt földi üvegszálas közeg (melyet költséges kiépíteni) helyett műholdakon keresztül történjen a kapcsolat, ráadásul nem csak egy műhold felhasználásával, hanem több műholdból álló műholdkonstelláció segítségével. Ebben a vizsgálatban az éppen fejlesztés alatt álló űrtávközlési rendszer, a Starlink ihletett, és néztem meg, mi lenne, ha ehhez hasonló rendszer adna otthont a kvantummoduloknak. Munkám során a több műholdon keresztül történő kvantumkulcsszétosztás hatékonyságát vizsgáltam.

Abstract

Today's safe communication mostly depends on the fact that the public key-based cryptography is hard to break using classical computers. Which is true since even for today's most powerful computers, it would take decades to decipher this type of encoding. But for nonconventional computers, e.g., a quantum computer, this process would only take seconds.

At the same time, using symmetrical-key-based cryptography can still provide us with the necessary amount of security in the world of working universal quantum computers. The only question is what kind of channel we can use to securely generate or distributes the necessary keys. This can be done by using a quantum key distribution protocol which is simple and well-functioning, but essentially it works point-to-point. With quantum key distribution systems connected in a network, we will start to talk about quantum internet. These are systems that not only are able to generate keys using quantum bits but are able to transport quantum information using fiber or free-space links.

During my work, I was simulating quantum communication systems. I simulated a system that connects two points on the Earth using sets of satellites. In these simulations, I was examining the possibility of instead fiber connections (which is expensive to build), using a series of

satellites. In my research, I was inspired by the underdevelopment Starlink and I looked at the possibility of using a system like that to host the quantum modules used for quantum key distribution.

1 Bevezetés

Kvantuminformatikával és kvantumkommunikációval, mint témával mindössze másfél éve találkoztam először témalaborom során és már akkor érdekelni kezdett a kvantumkommunikációs hálózatok és azok felépítése. Későbbi munkáim során kvantumhálózati szimulátorokon dolgoztam, majd azokon szerzett tudásomat felhasználva álltam neki kvantuminternet pont-pont szintű szimulációjához.

Amikor kvantuminternetről beszélünk, kétfajta megoldás járhat az eszünkben: az első megoldás egy kvantumcsatorna segítségével hoz létre két megegyező véletlenszerű bitsorozatot, két, egymástól akár több ezer kilométerre lévő pont között. Ez a szimmetrikus kulcs alapú kriptográfiára, és ennek következtében biztonságos kommunikációra is alkalmas. A második megoldás egy olyan rendszer létrehozása, ahol kvantuminformációt tudunk küldeni két pont között, ezzel kvantumszámítógépek hálózatát hozva létre. A kvantuminternetnek szükségszerűen nagy területet kell majd lefednie, innen jött számomra az ötlet, hogy a kvantuminternet gerincét sok száz műholdból álló rendszer képezze, mely által akár egész kontinenseket is lefedhetünk, minimális földi infrastruktúrával. Átalakítva egy létező kvantuminternet-szimulátor szoftvert azt vizsgáltam, hogyan lehet kulcsot megosztani nagyon sok műholdas csomópontot tartalmazó kommunikációs hálózaton. Két különböző alapelven működő hálózatot vizsgáltam: az egyik megbízható csomópontokat használ, a másik pedig nem megbízható csomópontokat

A fő célom a műholdascsomópont alapú rendszerek vizsgálatával, hogy egy képet kapjak azok lehetséges zavarairól és a zavart befolyásoló tényezőkről. Ezen információk által kaptam egy képet arról, hogy egy kiépítendő kvantuminternet esetén milyen nehézségeknek nézhetünk majd elébe. A szimulátorom futtatása előtt arra számítottam, hogy tapasztalt zaj és az ebből eredő hibaarány a köztes műholdcsomópontok számosságával nőni fog, ehelyett arra a következtetésre jutottam, hogy a zavar az útvonal hosszával nő.

A második fejezetben egy rövid áttekintést adok a kvantuminternet működéséről és kvantummechanikai alapjairól azon belül is kitérve az általam használt kvantummechanikai jelenségekre, mint például a kvantumösszefonódás és a kvantumösszefonódás-csere. A harmadik fejezetben ismertetem majd a NetSquid szimulátor felépítését és működését, beleértve annak moduláris felépítését. Végül a negyedik fejeztében ismertetem az általam fejlesztett szimulációs programot, amelyet a NetSquid „Chain Repeater” példakódjából fejlesztettem tovább, hogy alkalmas legyen műholdas csomópontokból álló hálózat kezelésére is. Számos szimulációs vizsgálatot végeztem el, amelyek eredményeit röviden ismertetem.

2 A kvantuminternet alapjai

2.1 Kvantummechanikai alapok

A kvantumkommunikáció és számítástechnika az időnk egyik leggyorsabban fejlődő ága. A legtöbb előrehaladás a kommunikáció, és titkosítás terén történt. A kvantumkommunikációra való igény nagyban a kvantumszámitógépek fejlődésének köszönhető, hiszen a bankok által is használt titkosítási módszer (RSA) könnyen feltörhető kvantum-algoritmusokkal (Shor algoritmusa) [1] és már csak a hardware fejlődése kell eljusson arra a szintre, hogy ezeket az algoritmusokat optimálisan ki tudjuk használni. Ahhoz, hogy szabadtéri kvantum-kulcsszétosztás működése és szükségessége könnyen megérthető legyen, szükség lesz a kvantummechanika egy egyszerűsített modelljére.

A kvantummechanika a mikroszkopikus dolgok működését és a látható világgal való kapcsolatát írja le, aminek az alapja a 4 posztulátum:

I. A zárt fizikai rendszer állapota olyan $|\phi\rangle \in H$ állapotvektorral írható le, amely komplex együtthatókkal rendelkezik, egységnyi hosszú a H Hilbert térben

II. A zárt rendszer időbeli változását unitér transzformációkkal írhatjuk le (amely csak az kezdő és végső állapotot ismerjük).

III. Legyen X a mérés lehetséges eredményeinek a halmaza. Egy mérés a mérési operátorok halmazával adható meg: $M = \{M_x\}, x \in X, M_x \in H$

Ha a rendszer állapota $|\phi\rangle$,akkor annak a valószínűsége, hogy a mérés x eredményt adja:

$P(X||\phi\rangle) = \langle\phi|M_x^T M_x|\phi\rangle$ *és a mérés után a rendszer állapota a következő lesz:*

$$|\phi\rangle' = \frac{M_x|\phi\rangle}{\sqrt{p_x}}$$

IV. Egy W kompozit (összetett) fizikai rendszer állapotát meg lehet állapítani az őt felépítő V és Y rendszerek szorzatából: $w = v \otimes y$, ahol $w \in W$, $v \in V$ és $y \in Y$.

A négy posztulátum az alapja a kvantummechanikának és minden azt felhasználó tudományágnak, mint például a kvantumkommunikációnak is. A négy posztulátumnak mérnöki megközelítésben a következőket tudjuk megfeleltetni.

Első posztulátum - kvantumbit

Második posztulátum - logikai kapuk

Harmadik posztulátum – kvantum állapotok mérése

Negyedik posztulátum - kvantumregiszterek.

A következő fontos elem, amire ki kell térni az a kvantum összefonodás. Az összefonódás egy különleges jelenség, amelynek megértéséhez szükséges a kvantumbit felírása: $|\phi\rangle = a|0\rangle +$

$b|1\rangle$ ahol ϕ a kvantumbit és ’a’ és ’b’ az egyes eredmények valószínűsége (az az mérés esetén mekkora eséllyel lesz 1 vagy 0). Az összefonódott párokat egyrészt nem tudjuk felírni két állapot tenzorszorzataként, másrészt az egyik tagon elvégzet mérés hatására a másik tag is felvesz egy (az összefonódott állapot által) meghatározott értéket, függetlenül attól, hogy a pár két tagja milyen nagy távolságra van egymástól.

Megvalósítását tekintve: összefonódott párokat elő tudunk állítani CNOT (controlled NOT) kapu segítségével. Összefonódott állapotok közül kiemelhetjük az úgynevezett Bell-állapotokat (vagy EPR párok). Ezek ortogonálisak egymásra, azaz méréssel meg lehet őket különböztetni egymástól. Ezek matematikai felírása sorrendben:

$$|\beta_{00}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\beta_{01}\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

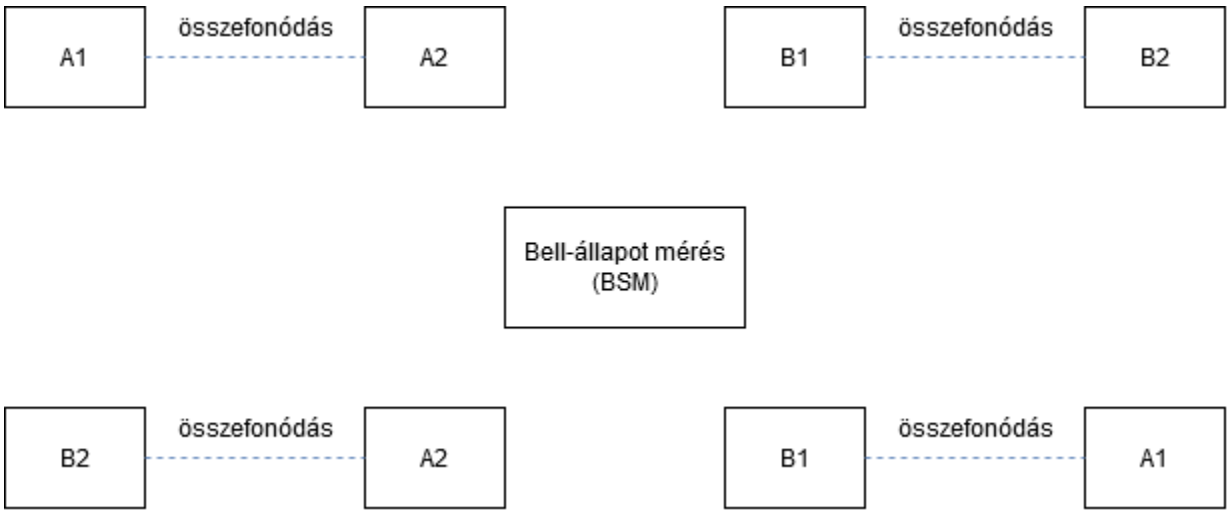
$$|\beta_{10}\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\beta_{01}\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

Amikor kvantumkommunikációban összefonódásról beszélünk, általában a fentebb említett párok valamelyikét használjuk. Az összefonódás a kvantumhálózatok egyik építőköve, és szerepet játszik a majd később részletesen tárgyalt E91 protokollban is.

2.1.1 Kvantumösszefonódás-csere

A kvantumösszefonódás-csere (entanglement swapping) egy fontos lépés volt a kvantumkommunikáció fejlődésében. Először a Genfi Egyetemen hajtották végre ezt a műveletet



1. ábra: Kvantumösszefonódás-csere BSM álltal. Fent a két összefonódott foton, alul pedig a már kicserélt összefonódással rendelkező fotonok találhatóak.

két, egymástól független, összefonódott fotonpáron (az ábrán A1-A2 és B1-B2). A1 és B1 fotonon végrehajtunk egy Bell-állapot mérést (Bell state measurment – BSM). A művelet után, mint az ábrán is láthatjuk, A1-B1 pár összefonódott állapotba kerül, ezt az egyetem kutatói mérésekkel igazolták is [2].

A BSM hatására a maradék két foton (A2 és B2), melyek eddig nem voltak egyszer sem kapcsolatba egymással, mint az ábrán is láthatjuk, összefonódtak, így az eredeti felállás összefonódásai „megcserélődtek”. Ezt a művelet ma már több protokollban is használják, például fel lehet használni az Artur Ekert alkotta E91 protokoll kiterjesztésében is ahhoz, hogy nagyobb távolságokat fedjünk le.

2.2 Kvantumkulcsszétosztás

A kvantumkulcsszétosztás során szimmetrikus kulcsú titkosíráshoz használandó kulcsokat osztunk meg kér kommunikáló fél, a küldő (Alice) és a fogadó (Bob) között. Emellett fontos megjegyezni, hogy az igazán biztonságos szimmetrikus kulcsú titkosításhoz (One Time Pad, OTP) egy kulcsot csak egyszer lehet használni, vagyis minden üzenethez külön kulcsot kell létrehozni. E két megegyező kulcs létrehozásához többféle QKD protokoll is létezik, a munkásságom során én kettőt használtam, a BB84-et és az E91-et. A QKD protokollokat többféle módon is lehet csoportosítani (első vagy második generáció, összefonódást használ vagy nem használ). Én egy harmadik csoportosítási módot használtam:

Megbízható csomópont (trusted node) esetén elvárjuk és feltételezzük, hogy maga a hardveres rendszer, ami a csomópontot alkotja nem rendelkezik olyan tulajdonságokkal, amely egy támadást lehetővé tenne.

Nem megbízható csomópont (untrusted node) egy olyan csomópont, ahol feltételezzük, hogy hardveres rendszer bármikor kompromittálódat és ez alapján tervezzük a protokollokat is.

2.2.1 BB84 protokoll

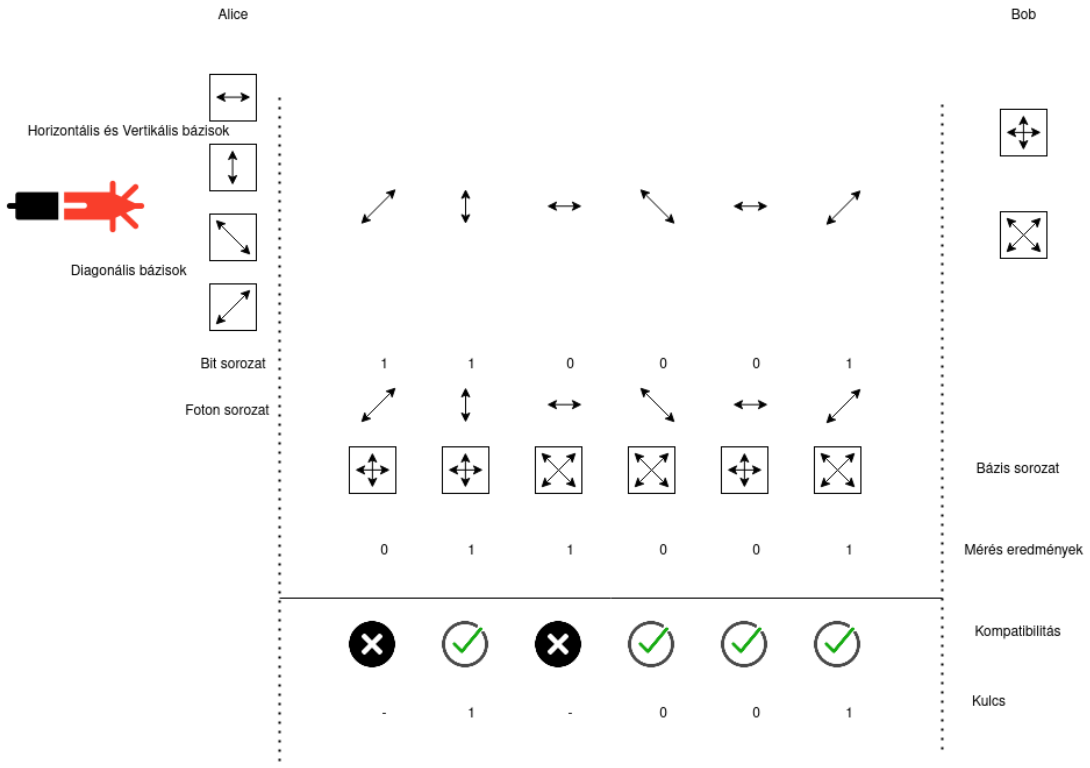
A BB84-et, az első kvantumkriptográfia-protokollt, 1984-ben alkotta meg Charles Bennett és Gilles Brassard [3]. A protokoll bizonyítottan biztonságos [3], hacsak a használt csomópont hardverre nem került egy rosszindulatú harmadik fél kezébe. Ebben az esetben a két végpont közötti kommunikáció lehallgatható lesz a két fél tudta nélkül. Mint protokoll részletes leírásánál látható, ez megoldás csak a két csomópont közötti lehallgatás ellen véd. A protokoll fő ismérve, hogy két féle mérési bázist is megkülönbözet: $|0\rangle$ és $|1\rangle$ vagy $|+\rangle$ és $|-\rangle$ állapotokat ($|+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}; |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$). A bit kódolási módját egy véletlenszám generátor kimenete fogja megadni.

A továbbiak során a következő jelölést fogom használni: Alice és Bob a két kommunikáló fél, Eve pedig a támadó.

2.2.1.1 Menete

A BB84 protokoll menetében 9 fő lépést különböztetünk meg, az utolsót részletesebben is ismertetem később.

1. Alice kiválaszt $(4 + \delta)n$ darab véletlenszerű adatbitet.
2. Alice kiválaszt még egyszer $(4 + \delta)n$ darab véletlenszerű bitet, ezt a sorozatot ezentúl *b*-nek hívjuk. Alice minden adatbitet kódol a hozzá tartozó *b* bittel. Ha *b* = 0 akkor $\{|0\rangle, |1\rangle\}$ és ha b = 1 akkor pedig a $\{|+\rangle, |-\rangle\}$ állapotba fogja kódolni.
3. Alice a kapott állapotot elküldi Bobnak.
4. Bob megkapja az $(4 + \delta)n$ darab állapotot, majd megméri őket az egyik vagy másik bázisban (ez véletlenszerűen lesz kiválasztva).
5. Alice egy publikus csatornán megosztja *b*-t.
6. Alice és Bob minden olyan bitet eldob, amit Bob rosszul mért, ez nagy valószínűséggel több lesz, mint 2*n* (ha a maradt bitek száma kisebb, mint 2*n*, akkor megszakítják a protokollt).
7. Alice kiválaszt *n* darab bitet, amelyeket arra fognak felhasználni, hogy az esetleges Eve általi lehallgatási próbálkozást észrevegyék. Ha több mint a megengedett számú bit eltér, akkor a protokollt megszakítják.
8. Alice és Bob végrehajtják az információösszeegyeztetését és a titkosításfelerősítését, amelyek segítségével megszerzik az *m* darab közös bitet.



2. ábra: Alice és Bob kommunikációja BB84 fölött. Látható Alice 4 polarizációs lehetősége és Bob 2 érzékelési bázisa. Kettejük között található egy kommunikáció lebonyolítása.

Az ábrán is láthatjuk, hogy lehallgatás esetén miért olyan könnyű azt észrevenni. A küldés pillanatában még nem tudott a *b*, így Eve nem tudja, hogy mely bázisban kellene elvégezni a mérését igy ő is csak véletlenszerűen választhat. Viszont Eve, mérése után is ugyan abban a bázisban kell tovább küldje az üzenetet Bobnak (vagy akár választhatná a másikat is szintén véletlenszerűen, itt a végkimenetelen nem változtatna).

2.2.1.2 Információösszeegyeztetés

Az információösszeegyeztetés az a módszer, ami által ki lehet szűrni az összes maradék eltérést a két kulcs között anélkül, hogy túl sok információt felfednénk róluk. Működésének lényege, hogy bitek csoportjainak a paritását hasonlítja össze Alice és Bob, majd minden összehasonlítás után a csoport utolsó bitjét kitörlik. Ezt a műveletet többször egymás után elvégzik így a végére nagy valószínűséggel mindketten ugyanazzal a kulccsal rendelkeznek, viszont, mivel ezt egy publikus csatornán végezték, Eve többlet információt kapott.

2.2.1.3 Titkosításfelerősítés

A titkosításfelerősítés módszerével lehet teljesen megszüntetni Eve bármely szintű tudomását, amit az információösszeegyeztetés alatt szerzett a kulcsról. Ehhez szükséges egy olyan modern hashelés melyre igaz, hogy kis változás is a bemenetben nagy változást vált ki a kimenetben. Egy ilyen hashelés például a SHA256 [4] [5].

2.2.2 E91 protokoll

Az E91 protokoll, amely Artur Ekert nevéhez fűződik, volt az egyik első olyan megoldás, mely a felhasználta az összefonódásban rejlő lehetőségeket. A BB84 és E91 protokoll között két nagy eltérés van: az első az, hogy az E91 protokollnak összesen csak annyira van szüksége, hogy Alice és Bob rendelkezzen egy összefonódott párral. Ebből következik a második eltérés, vagyis az E91 protokollnak nincs szüksége arra, hogy a köztes csomópontok is megbízhatóak legyenek [6].

2.2.2.1 Menete

Bemenet: Alice és Bob, akik szeretnének megosztozni *n* darab teljesen összefonódott kvantumbiten.

Erőforrások: Alice és Bob által használt publikus klasszikus kommunikációs csatorna

Cél: Alice és Bob létrehozzon egy közös titkos kulcsot

Protokoll:

1. Feltételezzük, hogy Alice és Bob a kvantumbitek mérését az $\{a_1,a_2,a_3\}$ és $\{b_1,b_2,b_3\}$ vektorok mentén tudja mérni, melyek megfelelnek a $\{|0\rangle, |1\rangle\}$ bázisnak elforgatva $\{0, \frac{\pi}{4}, \frac{\pi}{2}\}$ és $\{\frac{\pi}{4}, \frac{\pi}{2}, \frac{3\pi}{4}\}$ szögekben. Alice és Bob megméri a saját állapotaikat véletlenszerűen valamelyik vektor mentén.
2. Alice és Bob publikus csatornán kijelenti az álltaluk használt vektorokat, majd azokat az értékeket, ahol ugyanazt a vektort használták, félrerakják.
3. A fennmaradó eredményeket publikusan megosztják egymással és a belőlük számolt korrelációs érték alapján próbáljak detektálni a lehetséges lehallgatót.
4. Ha a korrelációs érték $S \approx 2\sqrt{2}$, akkor ki lehet jelenteni, hogy nem történt külső beavatkozás és a második lépésben félrerakott értékeket felhasználva létrehozzák a titkos kulcsukat.

2.3 Kvantuminternet

A kvantuminternet mint fogalom jelentősen el kezdett terjedni az utóbbi pár évben, olyan szinten, hogy ma már több ország is belekezdett a fejlesztésébe. Köztük olyanok, mint az Amerikai Egyesült Államok [7], az Európai Unió számos tagállama [8] vagy Japán [9]. A kvantuminternet terveknek két nagy táborát tudjuk megkülönböztetni aszerint, hogy a kvantumcsatorna két kvantumrendszert köt-e össze vagy két klasszikus rendszert. Az utóbbi esetben beszélünk például kvantumkulcsszétosztásról, míg az előbbi esetén egy tényleges kvantumhálózatról, ahol a kvantumszámítógépek képesek együttműködni akár nagy távolságokon keresztül is.

2.3.1 Összefonódáson alapuló kvantumhálózat különbsége a klasszikus hálózatokkal szemben:

1. Csomagok hiánya.

A kvantumhálózatok alapját az IP alapú hálózatokkal szemben nem csomagok képezik, hanem Bell párok. Ezeket mind egyenként kell kezelni, nem lehet hozzájuk fejlécet társítani. Ennek kiküszöböléséhez az eddig fejlécekben tárolt információkat klasszikus csatornán kell küldeni, amelyekhez majd a kvantumismétlőknek kell társítaniuk a kvantummemóriájukban tárolt kvantumbiteket.

2. Az összefonódott kvantumbit párok csak akkor hasznosak, ha mindkettő helyzetét pontosan tudjuk.

Mivel a pár egyik darabján végrehajtott művelet kihat a másik tagra is, ezért minden ilyen műveletet végző eszköznek nem csak tudnia kell, hogy hol helyezkedik el az adott kvantumbit párja, hanem a műveleteit össze is kell hangolnia az adott csomóponttal.

3. A kvantumkommunikációhoz szükséges az átmeneti állapot.

Míg a klasszikus csomagkapcsolt rendszerek esetén az adott csomag továbbküldése egy állapotmentes folyamat, addig a kvantumbithez tartozó információkra az adott eszköznek várnia kell, mivel mint az látható volt az 1. problémánál a kvantumbitek nem tartalmaznak semmilyen a kezelésükre vonatkozó kontroll információt. Így, míg az ehhez tartozó információt megkapja a kvantum csomópont, el kell mentenie a bit állapotát valamilyen módon.

2.3.2 Klasszikus kommunikáció:

A klasszikus kommunikációnak két fontos szerepe van a kvantuminternetben:

- Klasszikus bitek továbbítása, melyek szükségesek az elosztott protokollokhoz, mint az összefonódás-csere vagy a teleportálás
- Vezérlő információk közlése

A klasszikus kommunikációnak fontos szerepe van bármely kvantumhálózatban, hiszen, mint már fentebb említettem, a rendszer kontroll információinak egésze ezen az adatsíkon megy végbe.

2.3.3 A kvantuminternet elemei:

Kvantum routerek: kvantumismétlő vezérlő síkkal, ez az elem felelős a hálózat irányításáért és hogy előállítsa a megfelelő kvantumbiteket a kért végpont párokhoz. Rendelkezik a kvantumbitek tárolására alkalmas kvantummemóriával és a képességgel, hogy összefonódás cserét hajtson végre két kvantumbiten.

Automata kvantum csomópontok: csak az adatsíkot tartalmazza, nem vesz részt a hálózat irányításában, a no-clonning tétel miatt erősíteni nem lehet, így hosszú távok esetén több kvantumismétlő dolgozik együtt.

Végpontok: képes kell legyen fogadni kvantum párokat, viszont az automata csomóponttal szemben nincs szüksége sem kvantum memóriára, sem a képességre, hogy végrehajtson kvantum összefonodás cserét.

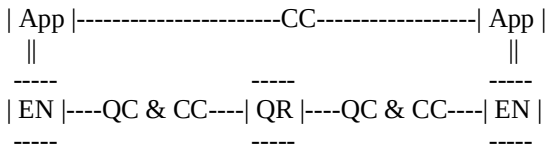
Nem kvantum csomópontok: nem mindegyik csomópontnak van szüksége kvantum adatsíkra, ez egy olyan csomópont, amely a klasszikus adatforgalmat kezeli.

Emellett kétfajta kapcsolatot fogunk megkülönböztetni:

Kvantum link: egy olyan link melyen keresztül tudunk a két összekötött kvantumismétlő között létre hozni egy összefonódott párt.

Klasszikus link: ezen keresztül küldjük a különböző klasszikus hálózaton is küldhető adatokat.

Egy két hoppos kvantumhálózat reprezentálható a következő módon:



App – felhasználói szintű alkalmazás
QR – kvantumismétlő
EN – végpont
QC – kvantumcsatorna
CC – klasszikus csatorna

1. táblázat: Egy kvantuminternetet használó alkalmazás absztrakt modellje és hálózati követelményei.

2.3.4 Fizikai kényszerek:

Memória életidők:

Mivel a kvantumcsatorna és a klasszikus csatorna közös munkája szükséges a kvantumbit továbbításához, a kvantumbitet várakoztatni kell, ehhez a művelethez pedig kvantummemória szükséges.

Összefonódási ráta:

Az összefonódási ráta, mely azt szabja meg hogy másodpercenként hány összefonódással kapcsolatos műveletet tud végrehajtani, egy szűk keresztmetszete a kvantum-kommunikációnak. Ez annak köszönhető, hogy a legtöbb implementáció is csak maximum 10Hz-en tudd működni.

Kommunikációs kvantumbit:

A kommunikációs kvantumbitek száma adja meg, hogy egyszerre hány párt tud generálni a rendszer [10].

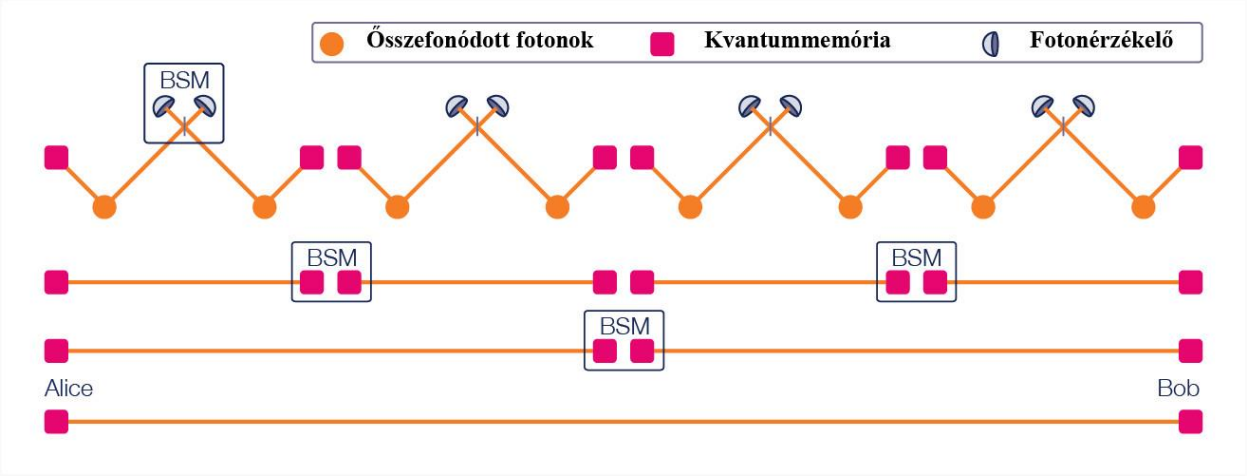
2.4 Kvantumkommunikáció fizikai felépítése

A kvantumkulcsszétosztás (quantum key distribution, QKD), mint rendszer, jelentősen eltér mind felépítésben mind működésben a klasszikus rendszerektől. Egy fizikailag is megvalósított QKD-rendszer több olyan elemmel is rendelkezik, amire ebben a dolgozatban nem térek ki. Köztük olyanok, mint a kvantum disztillációs csatorna, a kvantum szinkronizációs csatorna vagy a kvantumbitek különböző fajta implementációi.

2.4.1 Kvantumismétlő

Kvantumismétlőkre, mint elemekre, két okból van szükség: üvegszálas hálózatok esetében a küldött fotonok 150 km fölötti távolság esetén nagymértékben csillapodnak, így szükség van egy erősítőre. Erre viszont nincs lehetőség a kvantumbitek klónozhatatlansága miatt. A másik eset a szabadtéri kvantumcsatorna esetén áll fent, amikor is szükségünk van időnként nemcsak erősítésre, hanem irányváltoztatásra is (például műholdrendszerek esetén).

Az egyetlen probléma a kvantumbitek már fentebb említett klónozhatatlansága. Viszont, erre is van megoldás. Az ábrán is látható, hogy a rendszer hasonlít a klasszikus erősítő rendszerekre, miszerint a távolságot több kis részre osztjuk. A kvantumismétlő esetén viszont erősítők helyett kvantummemóriával felszerelt csomópontokat használunk, amelyeken kvantum-teleportációt hajtunk végre. Ebben az esetben nem információt, hanem az összefonódást teleportáljuk [11].



3. ábra: Alice és Bob kapcsolata több ismétlőn keresztül. A BSM a bell state measurment-et jelenti, ezt fentebb tárgyaltam a kvantumösszefonódás résznél. Az ábrán látható a szintén kvantumösszefonódás teleportálásnál említett kvantumbit csere is.

3 Kvantum hálózati szimulátorokok

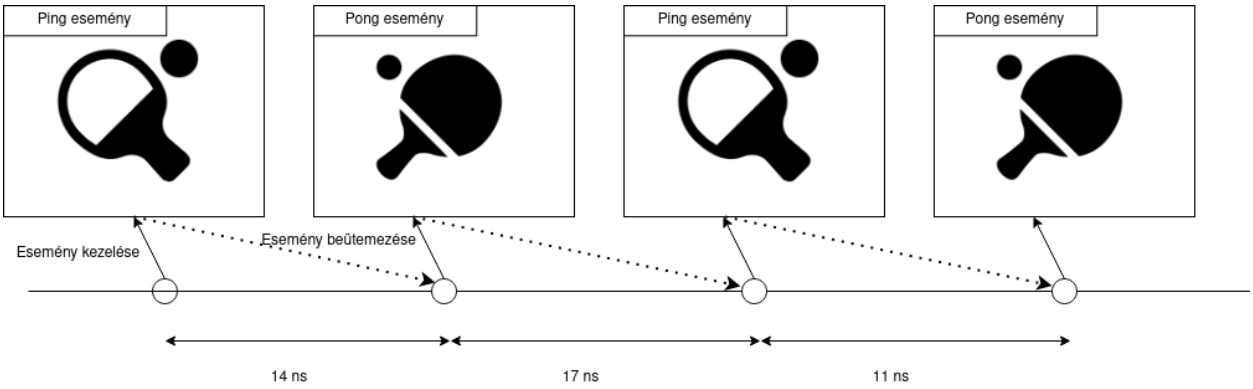
Munkám során megismerkedtem különböző kvantumhálózatokat szimuláló szoftverekkel, végül a választásom a NetSquid-ra esett, amit az alábbiakban röviden ismertetek.

3.1 NetSquid

A NetSquid (Network Simulator for Quantum Information using Discrete events) egy QuTech által fejlesztett szoftver, mely alkalmas skálázható kvantumrendszerek szimulálására [12]. A NetSquid fő előnye versenytársaival szemben, hogy képes pontosan modellezni az idő hatását egy kvantumrendszerben. Emellett egy nagyon részletes modellezési környezettel rendelkezik, melyben akár a kvantumprocesszor fizikai utasításait is meg lehet adni. A fejlesztők több példamodellt is közzétettek, így olyanok is készíthetnek szimulációkat, akik egyébként nem rendelkeznének egy ilyen részletes modell készítéséhez szükséges háttértudással.

3.1.1 Felépítése és működése

A rendszer egy diszkrét esemény vezérelt szimulátor, ahol az eseményeket előre ütemezi, majd a saját belső idejét a következő eseményhez igazítja. Ez az ábrán is nagyon jól látható, ahogy az esemény bekövetkezése következtében nem csak az események hajtódnak végre, hanem a következő esemény is előjegyzésre kerül.



4. ábra: A NetSquid esemény vezérelt rendszerének működési bemutatása. A szimulátor a belső idejét a következő ütemezett eseményhez igazítja.

A NetSquid csomag 5 alcsomagból épül fel (qubits, components, pydynaa, nodes, protocols), melyek szoros összedolgozásával jön létre a működő szimulátor. A csomagokat lehet külön is használni (persze a függőségek szem előtt tartásával). Moduláris felépítésének köszönhetően könnyedén meg lehet változtatni akár alapköveknek számító funkciókat vagy modulokat is anélkül, hogy ez a magasabb szintű rétegek működésében zavart okozna.

Későbbi fejezetekben leírt szimulációkhoz megadott paraméterek értelmezéséhez szükséges a szimulátor által használt hiba és depolarizációs modellek matematikai háttere. A kvantumprocesszorban található kvantummemóriában és kvantumkapukban fellépő zavar az egyik legnagyobb tényező a szimulátorban. Az ezeket leíró modellek figyelembe veszik, hogy az adott kvantumbit mennyi időt töltött a memóriában vagy a kapun áthaladva. Az egyenlet, amit modellek használnak egy 0 és 1 közötti számot adnak eredményül, mely annak a valószínűsége, hogy a kvantumbit depolarizálódik-e vagy sem. Ezt a következő módon számolja ki:

$P_{depol} = 1 - \exp(-időbeli\ eltolás\ [ns] * depolarízációs\ ráta\ [Hz] * 10^{-9})$ ahol a *depolarizációs ráta* a változó érték.

4 Műholdas kvantumkulcsszétosztó hálózat modellezése

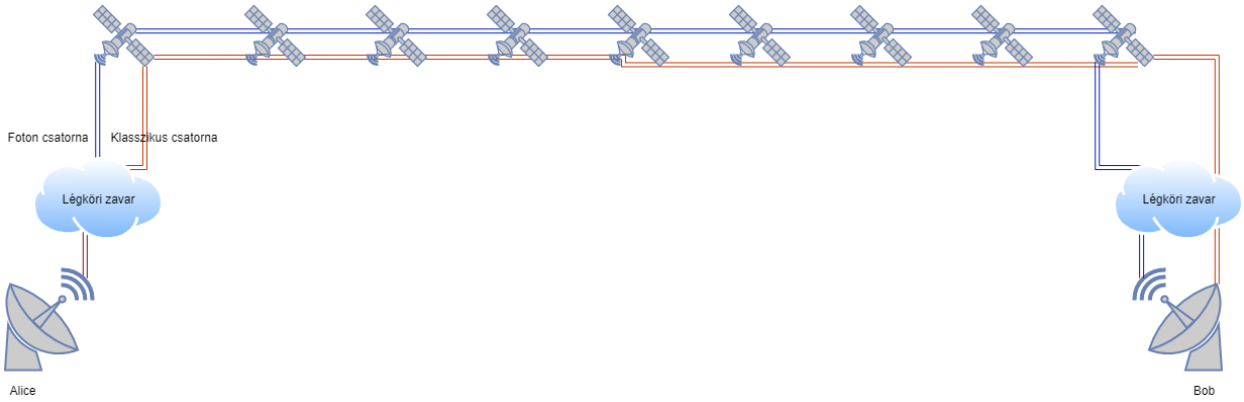
Munkám kezdetekor a fő célom, egy két felszíni pont közötti csatorna tulajdonságainak változásának követése volt a műholdak mozgásának függvényében. Ez a cél tovább fejlődött, nemcsak a csatorna adatait, hanem ezen csatornák használatával működő protokollok (nekem E91-re és BB84-re esett a választásom) működését is szimuláltam. Ugyan klasszikus és kvantum kommunikációt is tartalmazó rendszerrel dolgoztam, de munkám során főként a kvantumcsatorna tulajdonságaival foglalkoztam. Az alábbiakban saját fejlesztésű szimulátorral dolgoztam.

4.1 Szimulátor működése

A két protokoll szimulációja jelentősen eltérő, az alaprendszer mely a műhold adatokat szolgáltatja ugyan az. A műholdak helyzeteit a szimulátorban valós Starlink műholdak mozgása alapján modelleztem, így az eloszlásuk is hasonít a majd jövőben elkészülő Starlink rendszer tagjainak helyzeteire (annyi különbséggel, hogy ott már sokkal sűrűbben fognak elhelyezkedni, ezért más útvonaltervezési módszerekre lesz szükség a Dijkstra helyett).

4.1.1 Megbízható csomópontokon alapuló kvantumkulcs-szétosztás

A BB84 protokoll, bár a külső támadást könnyedén tudja érzékelni, de feltételezi, hogy a köztes csomópontok megbízhatóak. Ennek következménye, hogy az esetleges kvantumkommunikációs rendszerben való felhasználása esetén szem előtt kell majd tartani az egyes csomópontok kompromittálási esélyeit és azt, hogy ezeknek bekövetkeztével akár a teljes kommunikáció lehallgatható lesz.

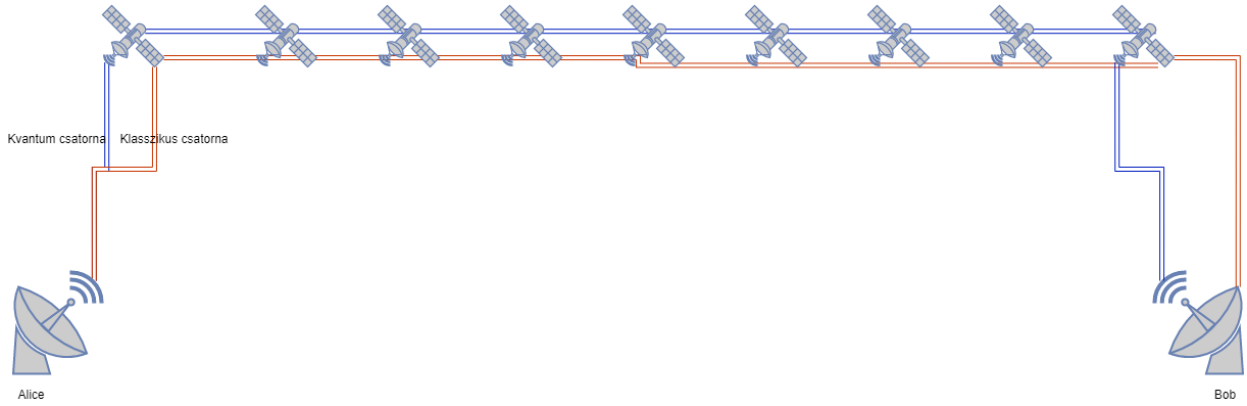


5. ábra: BB84 protokoll bemutatása két földi ponton keresztül. A légköri zavar nemcsak a fotoncsatornára, hanem a klasszikus csatornára is hat, bár az utóbbit egyszerű hibakódolással könnyedén ki lehet javítani.

Az ábrán is láthatjuk, hogy a légköri zavarok nemcsak a kvantumcsatornára, hanem a klasszikus csatornára is hatnak, bár az utóbbit egyszerű hibakódolással könnyedén ki lehet javítani. A szimulátor, mint a képen is látható, több műholdon keresztül szimulálja a csatorna adottságait és változásait. A műholdak helyzeteit és az azokon keresztüli útvonalat a később bővebben is kifejtett útvonaltervező- és műhold lekérdező modul hozza létre. Ezen adatok alapján számítja ki a légköri zavarmodell az teljes útvonal kvantum bithibaarányát.

4.1.2 Nem megbízható csomópontokon alapuló kvantumkulcs-szétosztás

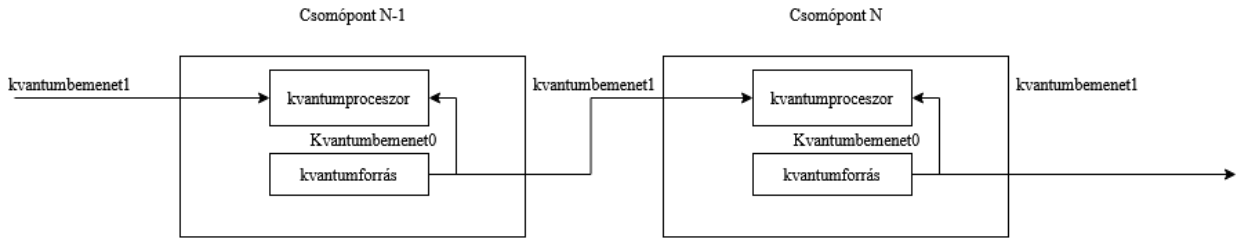
Az E91 protokoll fentebb leírt adottságainak köszönhetően a köztes csomópontoknak nem szükséges, hogy megbízhatóak legyenek, hiszen a szimmetrikus-kulcs létrehozásakor ellenőrizzük a lehetőséget, miszerint a támadó a csomópont felhasználásával próbálja a kommunikációt lehallgatni.



6. ábra: E91 protokoll csatornái két földi pont között.

A szimulátor működését jól szemlélteti a fentebb látható kép, egy több lépcsős, kvantum és klasszikus csatornákból álló hálózaton keresztül folytatja le Alice a kvantumkulcsszétosztást Bobbal, több műholdon keresztül.

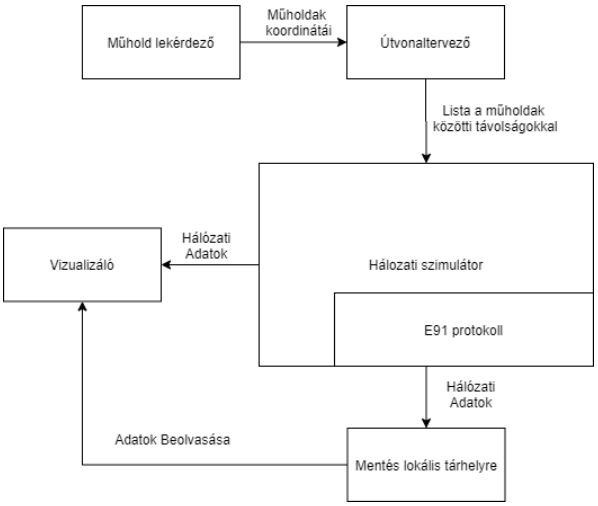
Az összefonódott kvantumbiteket Alice és Bob között egy úgynevezett összefonódás-cserével oldják meg a csomópontok. Mint azt az ábrán is láthatjuk, a csomópontok egy kvantumforrással vannak felszerelve, melynek segítségével hozzák létre a szomszédjaikkal az összefonódást.



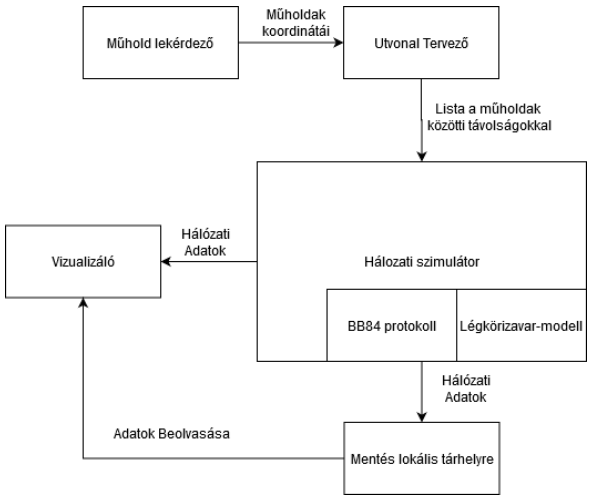
7. ábra: A kvantumismétlő csomópontok működése. A kvantumforrás egy-egy kvantumbitet küld az saját és a következő csomópont kvantumprocesszorának, ami segítségével létrehozzák az összefonódást.

4.2 A szimulációm felépítése

Az általam írt szimulátor egy továbbfejlesztése a NetSquid „Repeater chain” [12] példakódjának. Az eredeti szimuláció csak egy adott távon, egymástól egyenlő távolságra elhelyezkedő optikai kábellel összekötött kvantumismétlőket tudott szimulálni. A szimulátorom esetén a közeg nem optikai kábel, hanem légkör, ebből kifolyólag más zavarmodellel rendelkezik.



8. ábra: A nem megbízható csomópontokon alapuló szimulátor moduljai és azok közti kapcsolatai



9. ábra: A megbízható csomópontokon alapuló szimulátor moduljai és kapcsolatai

Mint a képen is látható, a szimuláció több fő modulból áll, melyek együtt dolgoznak a megfelelő működés érdekében. A modulok futás szerinti sorendben a következők:

Műhold lekérdező: Lekérdezi a Starlink műholdak helyzetét és annak változását a következő N másodpercre (N < 300), majd a kapott információt egy fájlba másolja, hogy onnan később is lekérdezhető legyen. A műholdak adatait a N2YO.com weboldalról kértem le [13].

Útvonaltervező: A kapott műhold koordináták és Dijkstra algoritmusa segítségével tervezi az útvonalat a hálózati szimulátortól kapott városok között. Miután meg van az útvonal, tovább küldi azt a szimulátornak.

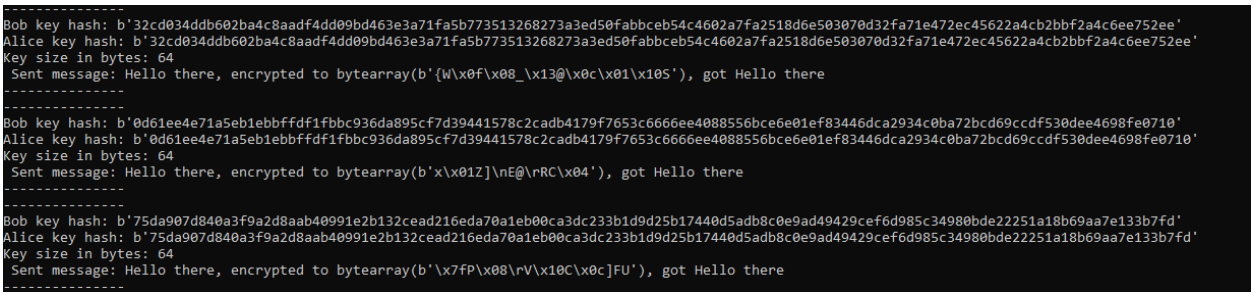
4.2.1 Megbízható csomópontokon alapuló kvantumkulcs-szétosztás specifikus modulok

Légkörizavar-modell: Az eddigi szimulációs modell, melyet használtam, bár pontos volt, a légkörben fellépő zavart nem szimulálta megfelelően, hiszen az eredeti példa kód zavar modelljét használtam, amely a közvetítő közeget optikai kábelként kezelte. Bár a szimuláció így is jó közelítő értéket adott, sajnos a valóságtól nagyon távol maradt. A hithű atmoszférikus modell leírásához szükséges információt egy műegyetemi atmoszférikus modellből [14] és a Kiss András-féle szimulációs fájlokból szereztem [15].

Maga a zavarmodell több dolgot is figyelembe vesz, melyet az eddig használt modell nem: nemcsak a levegőben megtett távolságot figyeli, hanem azt is, hogy az egyes légrétegekben mennyi idő alatt halad át a lézerjelünk. Ez fontos, hiszen a atmoszférikus szórás függ attól, hogy milyen

magaságban, éghajlaton és időjárásban helyezkedünk el. Fontos még, hogy a zavarmodell megkülönbözteti a föld-műhold és műhold-föld kapcsolatot is, ugyanis eltérő a nyalábszélesedés a két irányban.

BB84 protokoll modul: Ez a modul a már fent említett BB84 protokoll utolsó pár lépését hajtja végre a két felszíni pont között. Ezek közül a két fontosabb, a bevezetőben külön meg is említett, információösszeegyeztetés és a titkosításfelerősítés. Ezek által áll elő a biztonságos kommunikációhoz szükséges kulcs, melyet bár nem mentek el egy külső fájlba, de a mellékelt ábrán is látható a kapott kulcs pár és a küldött üzenet 3 állapota (küldés előtt, közben és után).



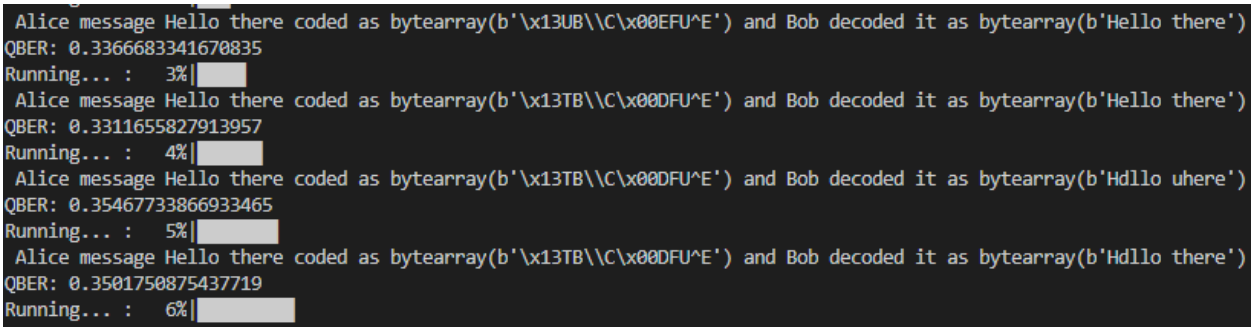
10. ábra: BB84 protokoll működés közben. Feltűnési sorrendben: Bob kulcsa, Alice kulcsa, kulcs mérete és az üzenet a küldés különböző fázisaiban

A protokoll titkosításfelerősítése által használt hash funkció implementáció függő, ez lehet bármely olyan funkció mely megfelelő mennyiségben eltérő kimenetet generál már kis bemeneti változás után is. A szimulációmban a SHA256 hash funkciót használtam a 256 bites kimenete miatt.

4.2.2 Nem megbízható csomópontokon alapuló kvantumkulcs-szétosztás specifikus modulok

Hálózati szimulátor: A szimulátor központi része, egy almodullal rendelkezik, mely az E91. Hálózati szimulátor modulban építettem fel a NetSquid segítségével a kvantumismétlő hálózatot az útvonaltervezőtől kapott távolságlista segítségével. Emellett, ebben a modulban találhatóak a protokollok és kvantumprocesszor utasítások, amik alapján működik az összefonódás-csere. A modul feladatai közé tartozik még a szimulációból az adatok rendszerezése és vizualizációra vagy mentésre való tovább küldése.

E91 protokoll modul: A modul összeegyezteti a különböző bázisban történt méréseket, így csak azok maradnak, amelyek ugyanabban a bázisban voltak mérve. Mivel itt a BB84-es protokollal szemben nem volt lehetősége egy külső támadónak a kulcsról bármi nemű információt szerezni, nincs szükség a fentebb látott információösszeegyeztetésre és a titkosításfelerősítésre, cserébe viszont időnként azt kell ellenőrizni, hogy egy támadó nem fonódott-e hozzá a rendszerünkhöz (Bell-állapotból GHZ-állapotba léptetve a rendszerünket). Az ábrán látható, hogy az üzenetet sikeresen lehet dekódolni a Bob által birtokolt kulccsal. Fontos még megjegyezni, hogy a depolarizációból eredő bithibákat egy stabilabb kommunikáció érdekében érdemes semlegesíteni bármely ma már ismert és széleskörben használt bithibakódolással.



11. ábra: E91 protokoll működés közben. Az ábrán látható Alice üzenete, a kódolt üzenet, majd annak a Bob által dekódolt verziója

4.3 Számítási modellek

4.3.1 Megbízható csomópontokon alapuló kvantumkulcs-szétosztás specifikus számítási modellek

A BB84 protokoll esetében a legnagyobb zavar a légkörön való áthaladásból származik, ezt a már fentebb bemutatott légkörizavar-modell segítségével számítottam ki, olyan tényezők figyelembevételével, mint a légkör tisztasága, az adott évszak, a műhold és az adóállomás/vevőállomás által bezárt zenitszög, lásd. részletesen az 2. táblázatban. A végső eredményt a következő számítás elvégzésével kaptam:

$$QBER = totalNoise * \frac{4}{staticLoss * dynamicLoss}$$ ahol a totalNoise $2 * 10^{-7}$

Légkör állapota	Tiszta-Ködös
Évszak	Nyár-Tél
Vevőállomás-műhold által bezárt zenszög	$0° - 90°$
Két pont közötti távolság	$0 - 4620\ km$
Detektor hatásfoka	$0{,}5 - 1{,}0$
Tükör átmérője	$0{,}5 - 2{,}0$ méter

2. táblázat: a BB84 zavarmodellje által használt paraméterek és tartományaik

4.4 Eredmények

4.4.1 BB84

A BB84 szimulációt több útvonalon (Budapest-Moszka, Budapest-Tokió, Budapest-New York) és több különböző bemeneti paraméterrel is lefuttattam. Itt a legtöbb változtatást a légkörizavar-modellen belül tudtam végrehajtani. Ezért a szimulációk eredményeiben a következő paraméterek lesznek feltüntetve:

Detektor hatásfoka (quantum efficiency) [0,5-1]: mekkora valószínűséggel érzékeli a fotont a detektorunk

Évszak [nyár-tél]

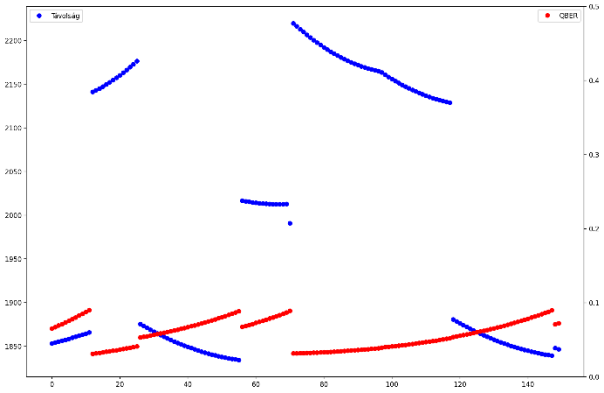
Időjárás [tiszta-ködös]

Tükör átmérője [0,5-2,0 méter]

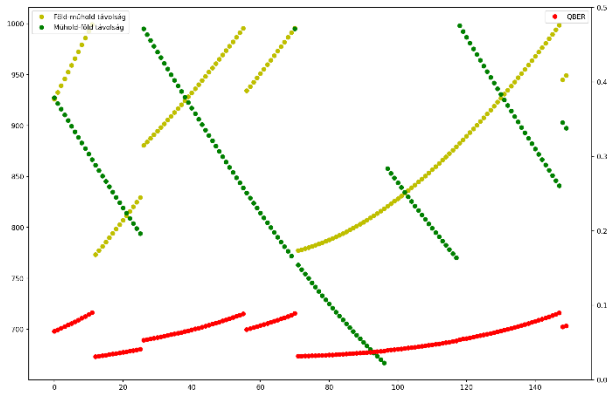
4.4.1.1 Kulcsszétosztás téli, ködös időben

Detektor hatásfoka: 0,7; Évszak: tél; Időjárás: ködös; Tükör átmérője: 0,5 méter

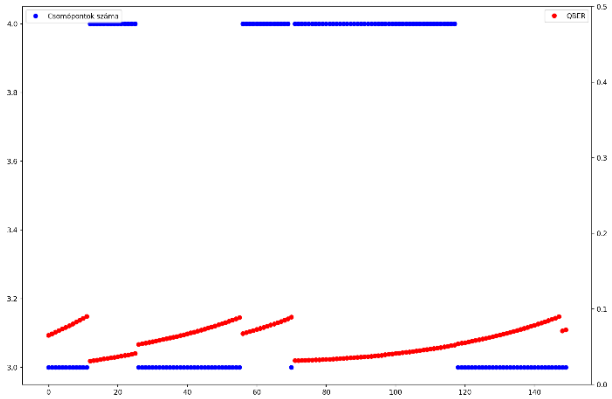
Budapest → Moszkva



12. ábra: Kvantum bithibaarány a távolság függvényében. Az ábrán kéken láthatjuk az útvonal hosszát az adott időpillanatban, az ehhez tartozó értékek a függőleges tengely bal oldalán láthatóak. A tengely jobb oldalán a kvantum bithibaarány található, melyhez a tartozó pontok piros színnel szerepelnek. Az adott útvonalat minden másodpercre újra számolja a szimulátor, majd végrehajt rajta egy teljes szimulációt. Az útvonal hosszában bekövetkezett hirtelen ugrások oka, hogy az adott műhold belépett a Föld árnyékolásába.

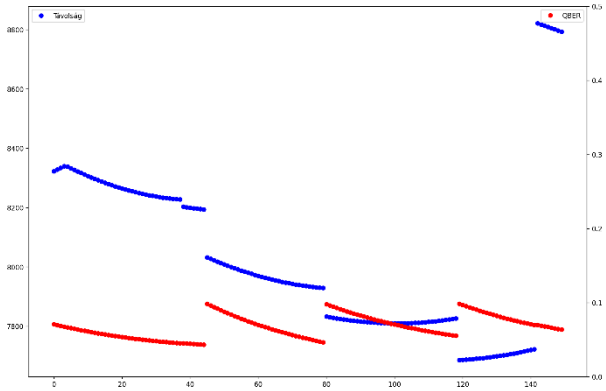


13. ábra: Kvantum bithibaarány a föld-műhold és műhold-föld útvonal függvényében. Az ábrán a föld-műhold és műhold-föld sárgás- és sötét zölddel ábrázolva látható, a hozzá tartozó értékek a bal függőleges tengelyen találhatóak. A tengely jobb oldalán a kvantum bithibaarány látható, melyhez a tartozó pontok piros színnel szerepelnek. Az adott útvonalat minden másodpercre újra számolja a szimulátor, majd végrehajt rajta egy teljes szimulációt. A szimuláción látható, hogy inkább a föld-műhold és az műhold-föld úton fellépő távolság növekedés hat ki a kvantum bithibaarányra. Ennek oka, hogy a távolság növekedése (mivel a műholdak egy konstans magasságon tartózkodnak), egyben a zenittel bezárt szög növekedését is jelenti, melyből kifolyólag nagyobb légkör tartományon kell a lézernek keresztül haladnia és ennek köszönhetően nagyobb lesz a zavar is.

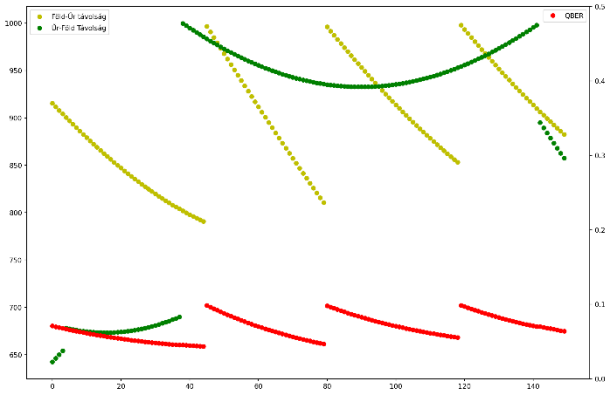


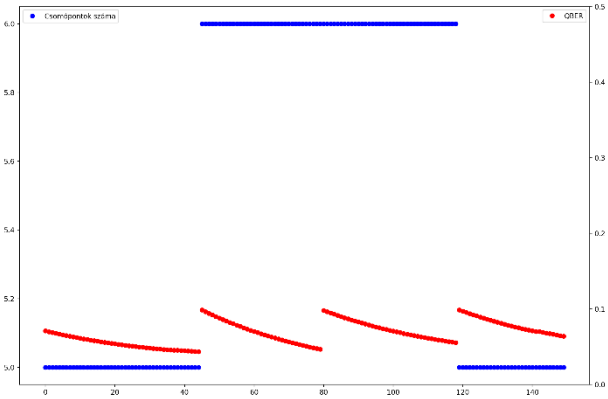
14. ábra: Kvantum bithibaarány a csomópontok mennyiségének függvényében. Az ábrán kéken látható az útvonalat képező csomópontok száma, a pontos értéket a baloldali függőleges tengelyen láthatjuk. A tengely jobb oldalán a kvantum bithibaarány található, melyhez a tartozó pontok piros színnel szerepelnek.

Budapest → New York

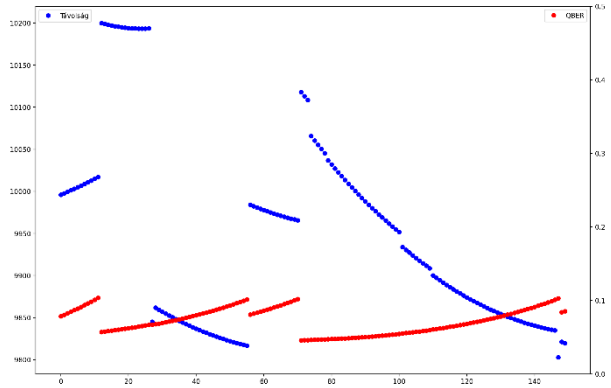


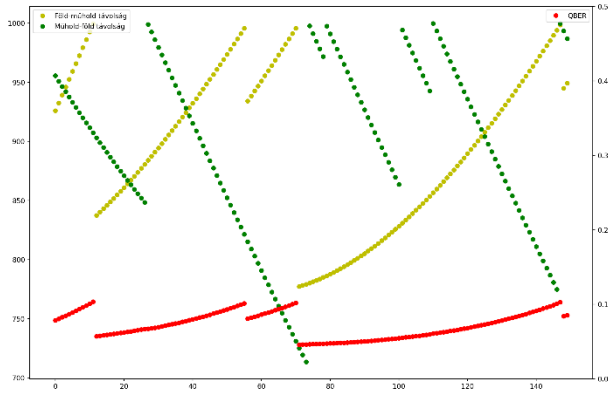
15. ábra: Az útvonal hosszában bekövetkezett hirtelen ugrás oka, hogy az adott műhold belépett a Föld árnyékolásába.

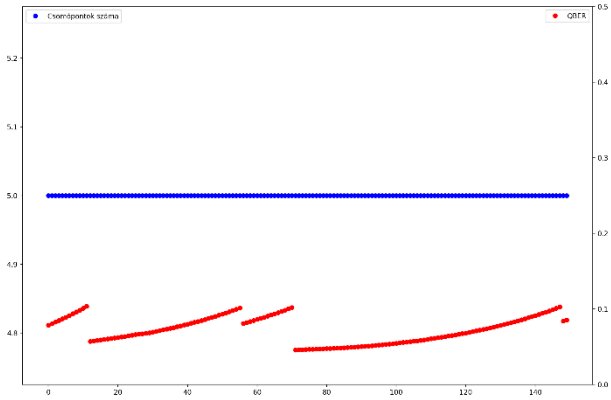




Budapest → Tokió



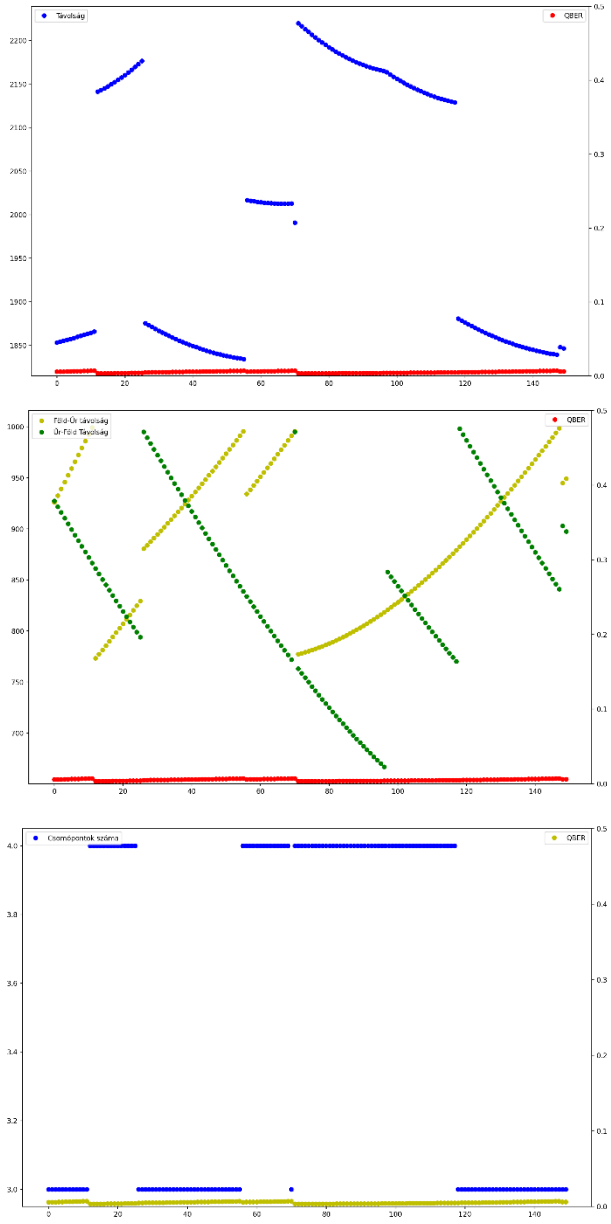




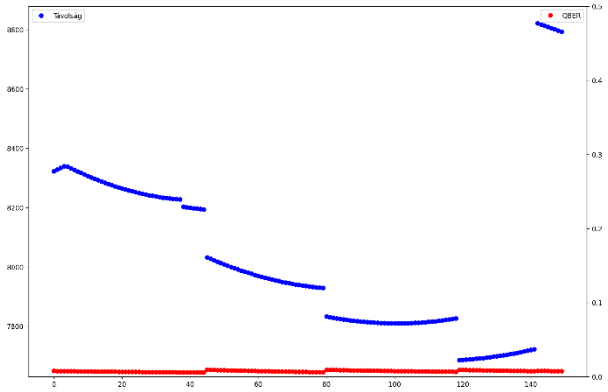
4.4.1.2 Kulcsszétosztás nyári, tiszta időben

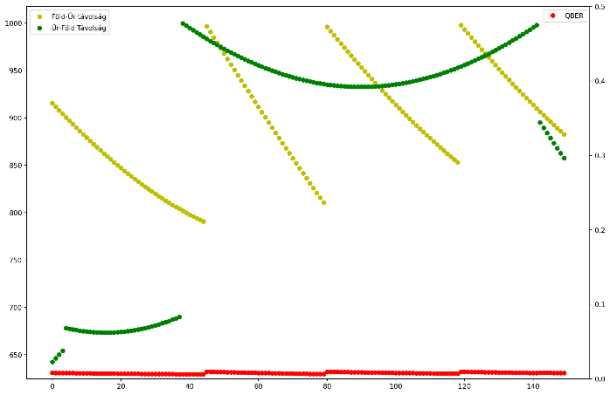
Ebben a szimulációban az alábbi paraméterekkel dolgoztam: Detektor hatásfoka: 0,7; Évszak: nyár; Időjárás: tiszta; Tükör átmérője: 1 méter. (Az első szimulációval összehasonlítva nem csak az időjárási körülmények változtak, hanem a tükör átmérőjét is megnöveltem.)

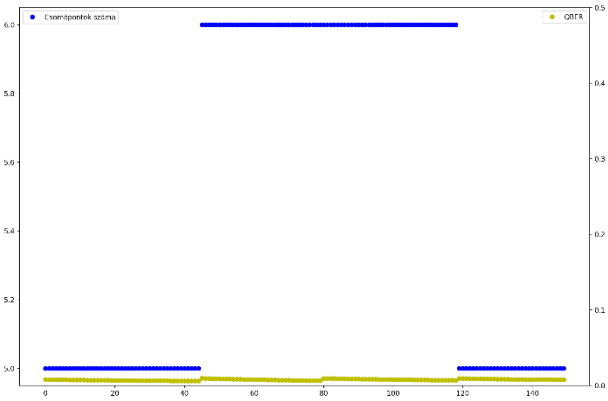
Budapest → Moszkva



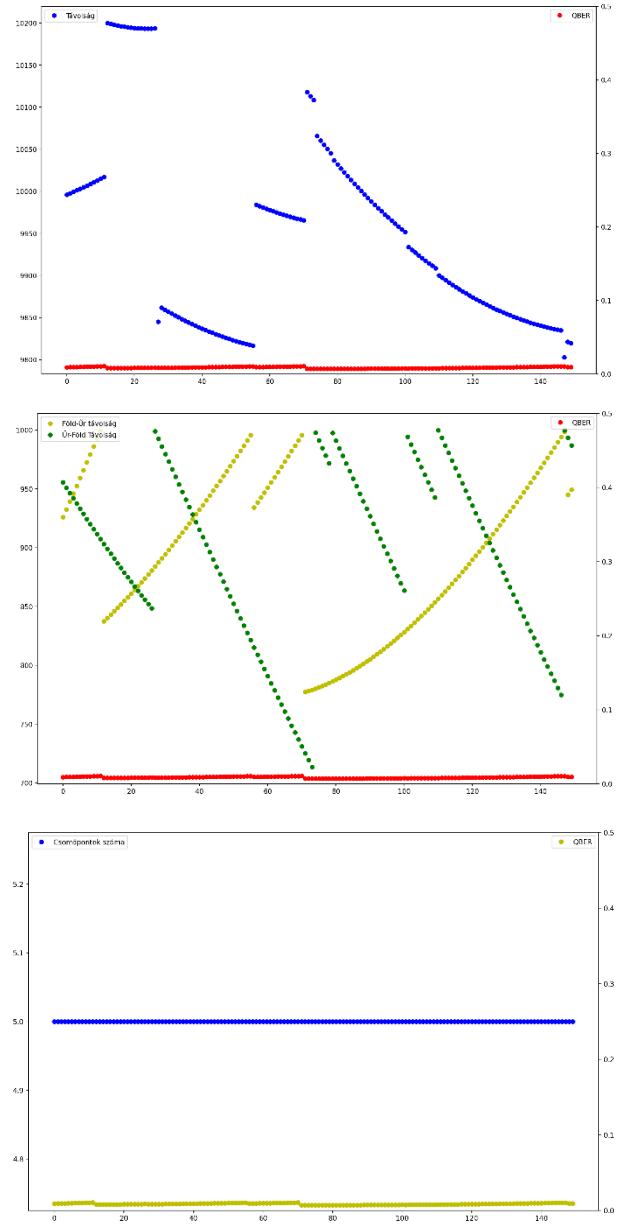
Budapest → New York







Budapest → Tokió



A fenti ábrákon jól megfigyelhető, hogyan befolyásolja a kvantum bithibaarányt nagyobb a föld-műhold és műhold-föld útvonalon fellépő távolság növekedés. Emellett az is látható, hogy a tükör méretének növelésével és jobb légköri körülmények hatására a kvantum bithibaarány jelentősen lecsökkent.

4.4.2 E91

Összefonódáson alapuló kvantumkulcszétosztás vizsgálatához az E91 protokollt választottam. A szimulációk során már kevesebb paramétert változtattam. Ezek név szerint: a kvantummemória depolarizációs rátája [Hz], kvantumkapuk fázisszétfolyás rátája [Hz] és késleltetése [ns]. A kvantumkapuk késleltetését három kategória szerint adtam meg aszerint, hogy milyen típusú felépítést követnek. Ezek sorrendben: szupravezető, ion csapda és semleges atomok. Az áthaladási időket a mellékelt [16] kutatásból vettem, melyeket az alábbi ábrán is láthatjuk.

Gate	Superconductors	Ion Traps	Neutral Atoms
CNOT	22	120,000	11,370
SWAP	17	10,000	34,120
H	6	6,000	2,991
$\|+\rangle$ prep.	100	16,000	3,991
$\|0\rangle$ prep.	106	10,000	1,000
X meas.	16	106,000	82,991
Z meas.	10	100,000	80,000
X	10	5,000	2,667
Y	10	5,000	2,667
Z	1	3,000	5,532
S	1	2,000	3,125
T	1	1,000	3,125

16. ábra Különböző kvantum kapuk felépítés szerinti késleltetése. [16]

A protokoll sajátosságai miatt, a legtöbb zavar a kvantummemóriából és kvantumkapukból kifolyólag keletkezik. Viszont ezek közül jelenleg csak a szupravezető űrkvalifikált technológia, a többi sajnos nem az, így a továbbiakban csak az erre épülő kvantumkapu modelleket fogom használni szimulációim során.

Kvantummemória depolarizációs zavar frekvenciája [0-90 Hz]

Kvantummemória fázisszétfolyás rátája *200*

Kvantumkapuk fajtái [Szupravezető]

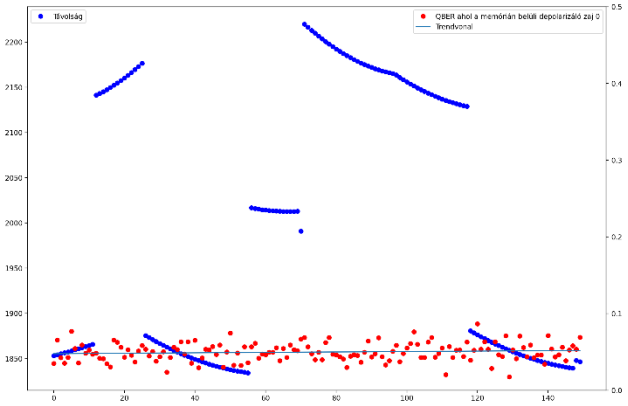
4.4.2.1 Kulcsszétosztás iteratívan növekvő depolarizációs zajban, Budapest és Moszkva között

Ebben a szimulációban a következő paraméterekkel dolgoztam: *Kvantum depolarizációs zavar frekvenciája: 0-90 Hz; Kvantummemória* fázisszétfolyás rátája*: 200 Hz; Kvantumkapuk fajtái: Szupravezető. (A depolarizációs zajt csak a kvantummemórián belül növeltem)*

Zavar mértéke [Hz]

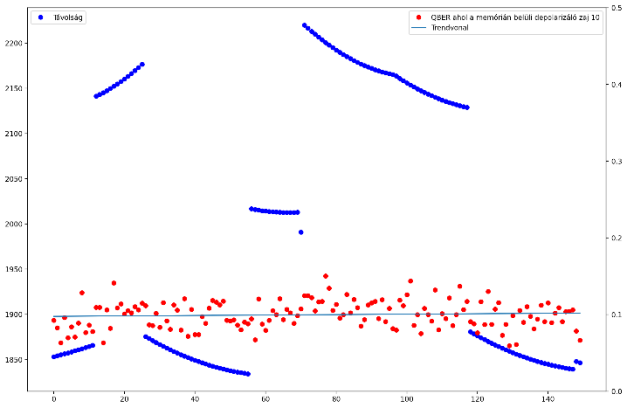
Budapest →Moszkva

0 Hz



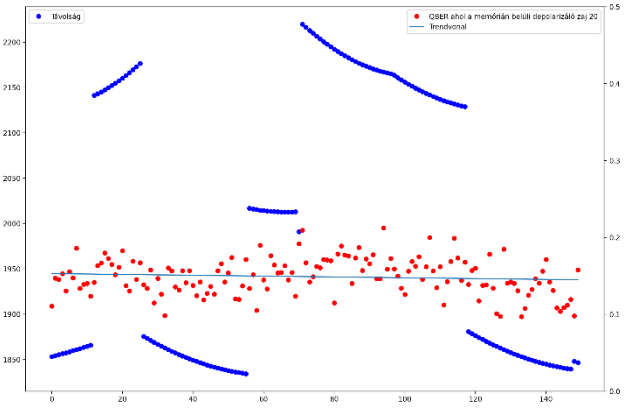
17 ábra: Kvantum bithibaarány a távolság függvényében. Az ábrán kéken láthatjuk az útvonal hosszát az adott időpillanatban, az ehhez tartozó értékek a függőleges tengely bal oldalán láthatók. A tengely jobb oldalán a kvantum bithibaarány található, melyhez a tartozó pontok piros színnel szerepelnek, emellett látható még a hozzá tartozó trend vonal is. Az adott útvonalat minden másodpercre újra számolja a szimulátor, majd végrehajt rajta egy teljes szimulációt. A képen lehet látni, hogy ha a memóriában szereplő zavar 0, akkor a kvantum bithibaarány is nagyon alacsony marad az egész szimuláció ideje alatt.

10 Hz

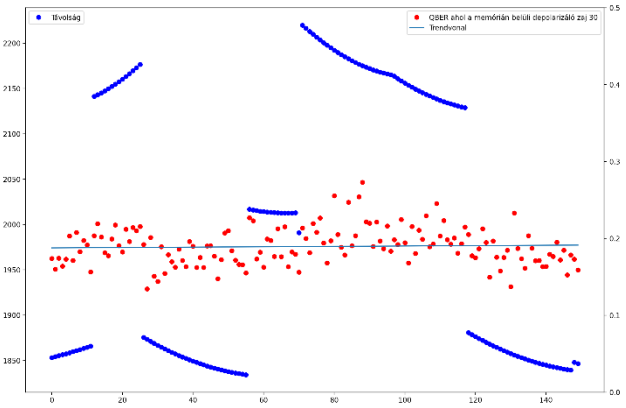


18. ábra: Depolarizációs zaj megjelenésével a kvantumbithiba-arány is elkezd növekedni. Megfigyelhető a 80. másodperc környékén egy kisebb eltérés a trendtől, a későbbi képeken tisztán lehet látni, hogy ennek az oka a távolság növekedése.

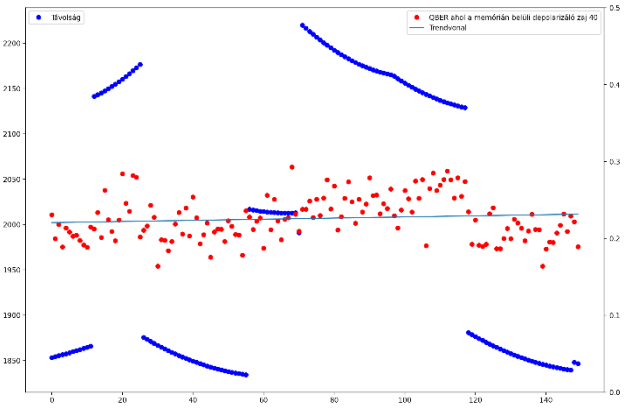
20 Hz



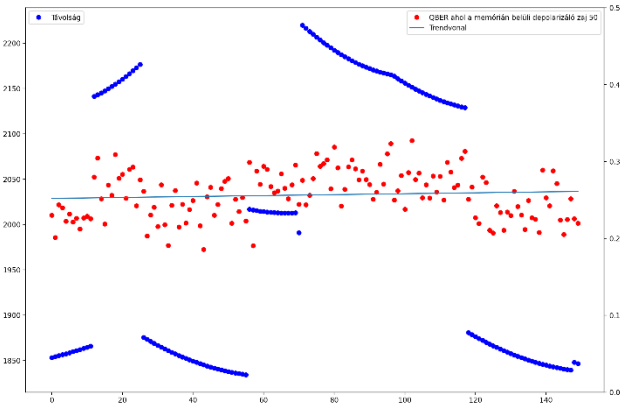
30 Hz



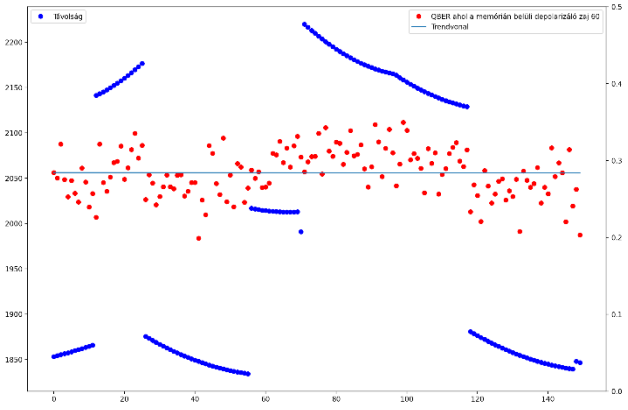
40 Hz



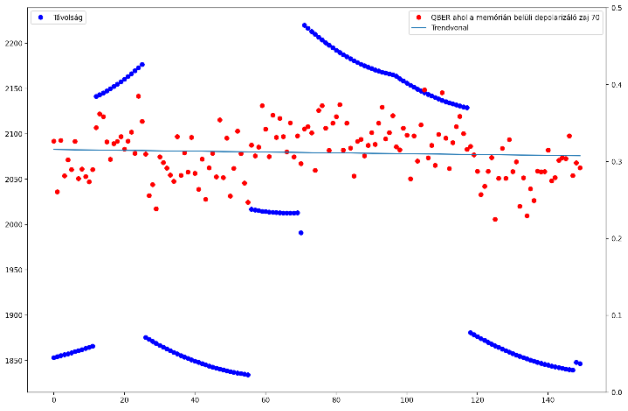
50 Hz



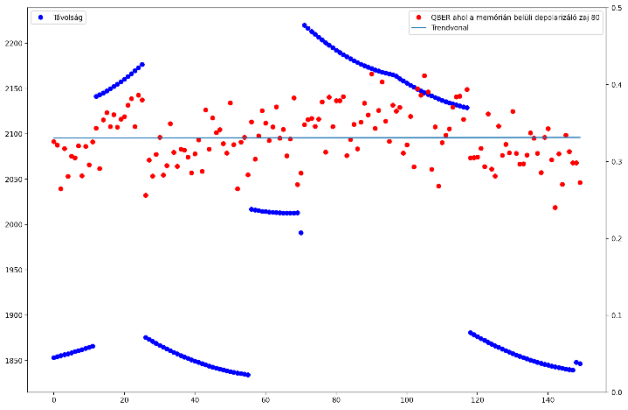
60 Hz



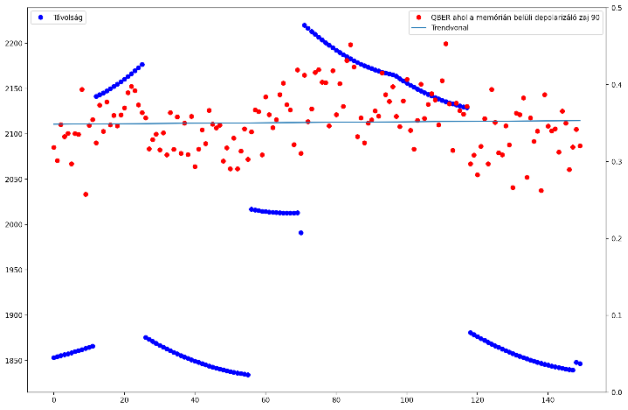
70 Hz



80 Hz

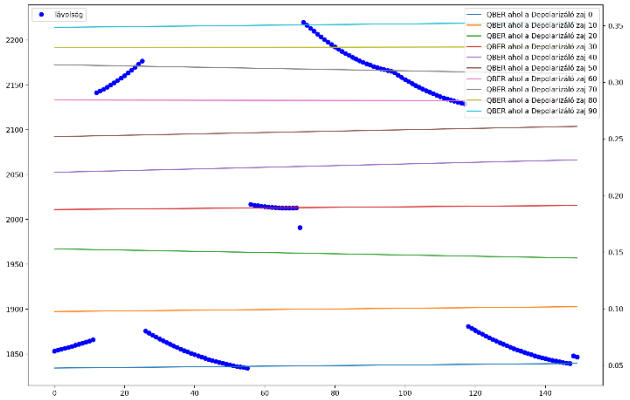


90 Hz



19. ábra: Ezen az ábrán már sokkal jobban kivehető a fentebb említett észrevétel, miszerint a kvantum bithibaarány megnövekszik, ha a távolság is nő.

Aggregált



20. ábra: Összes szimulált kvantum bithibaarány trend a távolság függvényében. Az ábrán kéken láthatjuk az útvonal hosszát az adott időpillanatban, az ehhez tartozó értékek a függőleges tengely bal oldalán láthatók. Kvantum bithibaarány trendvonalait láthatjuk sorban ábrázolva, a hozzájuk tartozó értékek a függőleges tengely jobb oldalán találhatók.

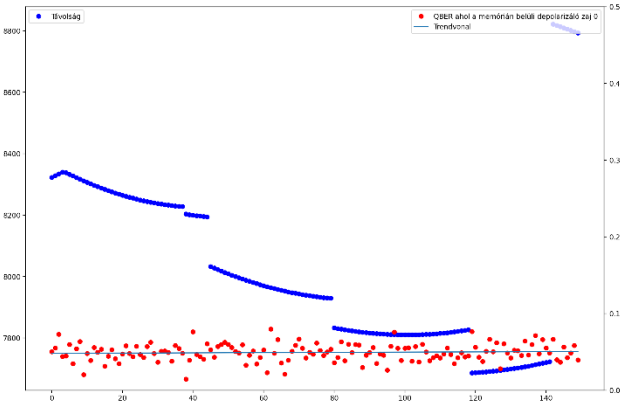
4.4.2.2 Kulcsszétosztás iteratívan növekvő depolarizációs zajban, New York és Budapest között

Ebben a szimulációban a következő paraméterekkel dolgoztam: *Kvantum depolarizációs zavar frekvenciája: 0-90 Hz; Kvantummemória* fázisszétfolyás rátája*: 200 Hz; Kvantumkapuk fajtái: Szupravezető. (A depolarizációs zajt csak a kvantummemórián belül növeltem)*

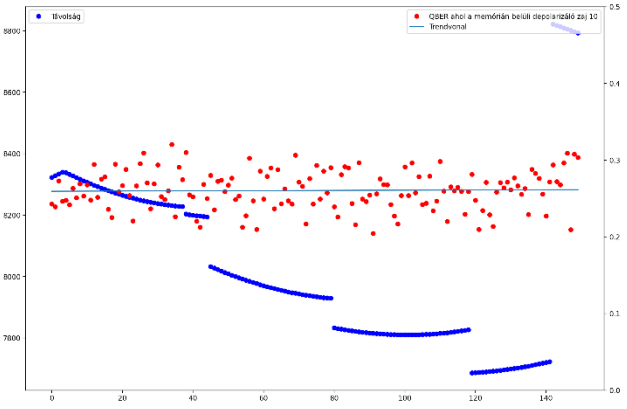
Zavar mértéke [Hz]

New York →Budapest

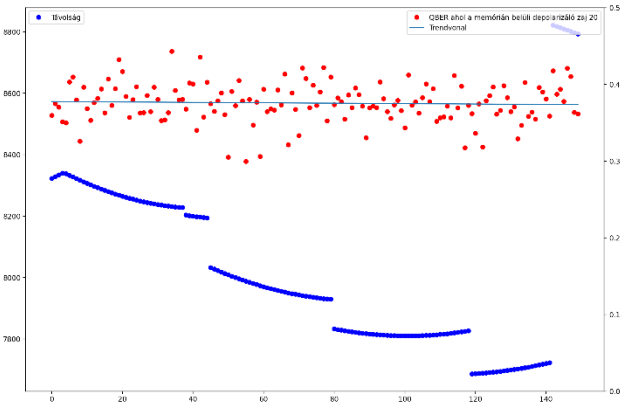
0 Hz



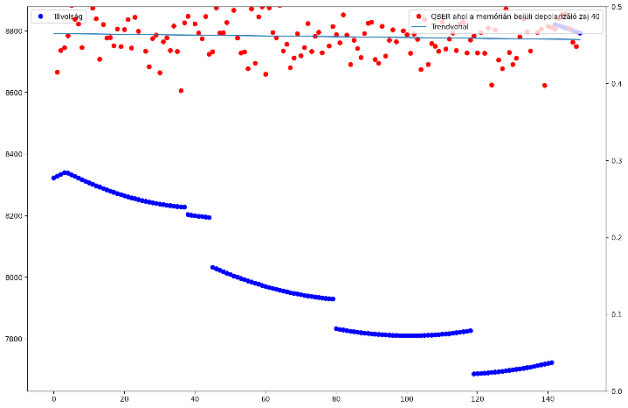
10 Hz



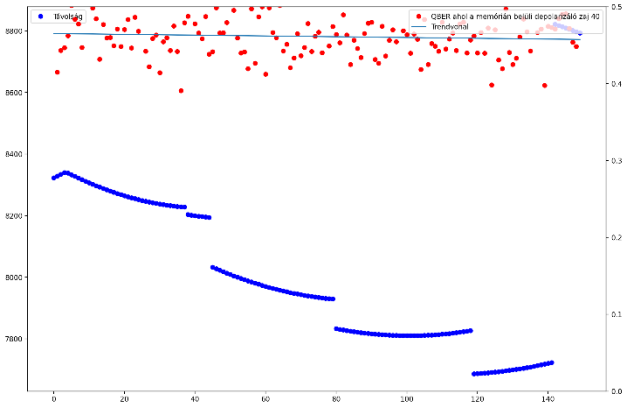
20 Hz



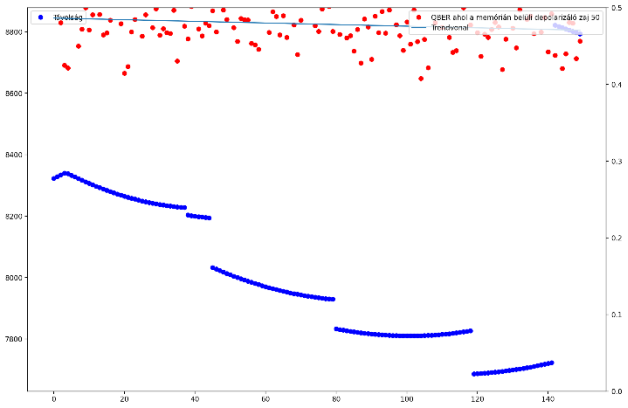
30 Hz



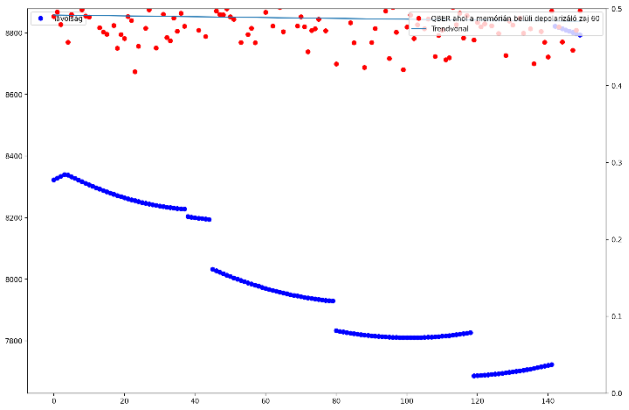
40 Hz



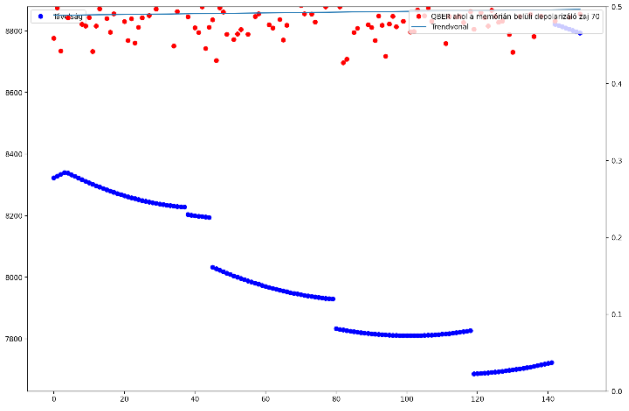
50 Hz



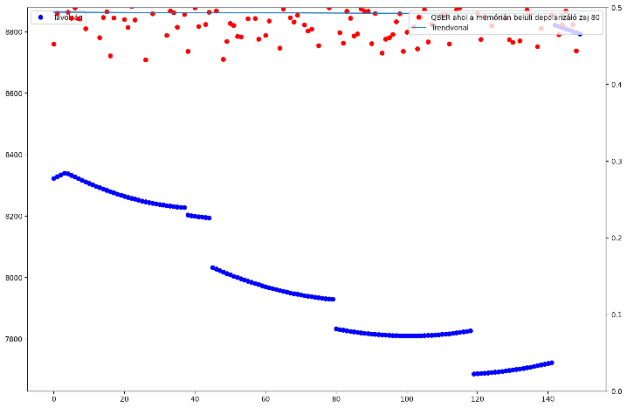
60 Hz



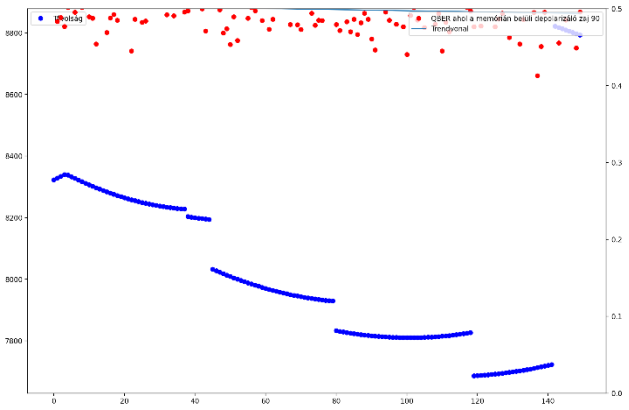
70 Hz



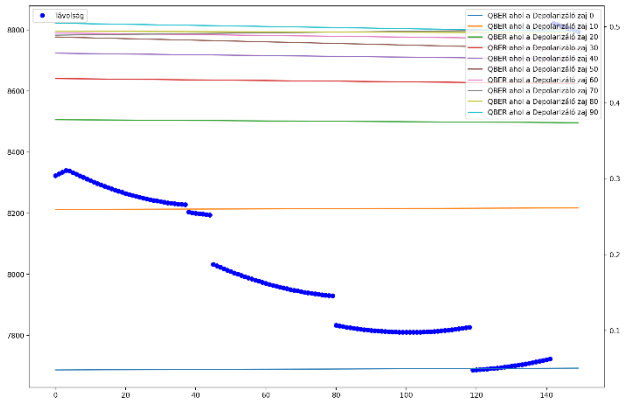
80 Hz



90 Hz



Aggregált



A fenti ábrákon jól megfigyelhető, hogy a kvantumkapu depolarizációs rátája a távolság függvényében hat a kvantumbithibaarányra. Azaz egy adott depolarizációs ráta esetén a távolságban bekövetkezett növekedés/csökkenés a kvantumbithibaarányt is növeli/csökkenti.

4.4.3 Csomópontok száma és távolság hatásai – E91

A valós adatokon való szimuláció mellet fontosnak tartottam, hogy összehasonlítsam az útvonal hosszának és a csomópontok számának növekedését, úgy, hogy a másik érték konstans marad a szimuláció során.

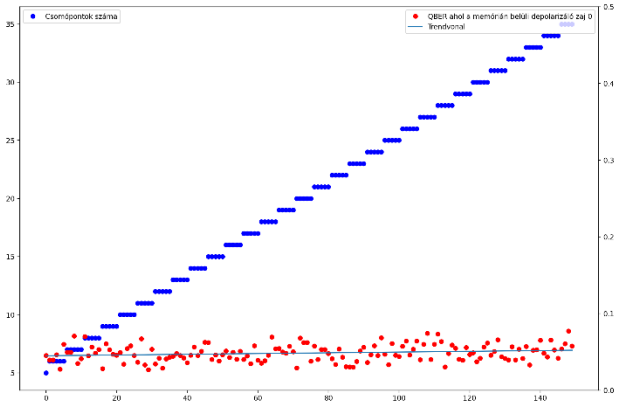
4.4.3.1 Kulcsszétosztás iteratívan növekvő depolarizációs zajban, időben növekvő számú csomópontok között

Ebben a szimulációban a következő paraméterekkel dolgoztam: *Kvantum depolarizációs zavar frekvenciája: 0-90 Hz; Kvantummemória* fázisszétfolyás rátája*: 200 Hz; Kvantumkapuk fajtái: Szupravezető. (A depolarizációs zajt csak a kvantummemórián belül növeltem)*

Zavar mértéke [Hz]

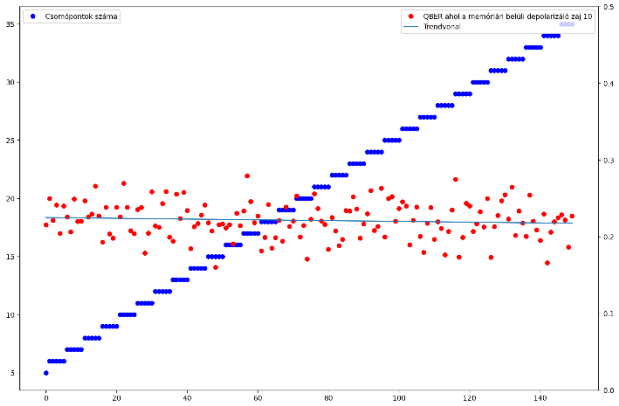
Csomópontok száma

0 Hz



21. ábra: Kvantum bithibaarány a csomópontok számának függvényében. Az ábrán kéken láthatjuk a csomópontok számát az adott időpillanatban, az ehhez tartozó értékek a függőleges tengely bal oldalán láthatók. A tengely jobb oldalán a kvantum bithibaarány található, melyhez a tartozó pontok piros színnel szerepelnek, emellett látható még a hozzá tartozó trend vonal is. Az adott útvonalat minden másodpercre újra számolja a szimulátor majd végrehajt rajta egy teljes szimulációt. A képen lehet látni, hogy ha a memóriában szereplő zavar 0, akkor a kvantum bithibaarány is nagyon alacsony marad az egész szimuláció ideje alatt.

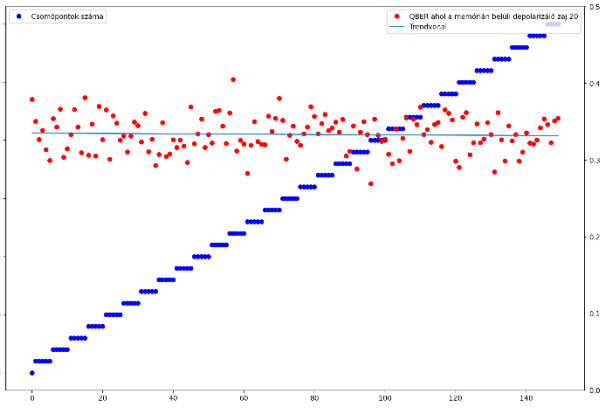
10 Hz



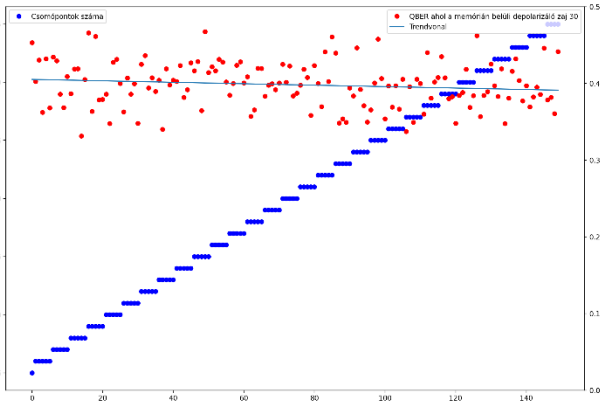
22. ábra: Észre lehet venni, hogy mint azt ahogy az előző szimulációkban is tapasztaltuk, a kvantum bithibaarányra legjobban a depolarizációs

zavar ráta és a távolság együttese hat. Az alábbi ábrákon lehet majd látni, hogy a depolarizációs zavar rátájának növelése csak „feljebb tolja” a kvantumbithiba arány trendvonalát.

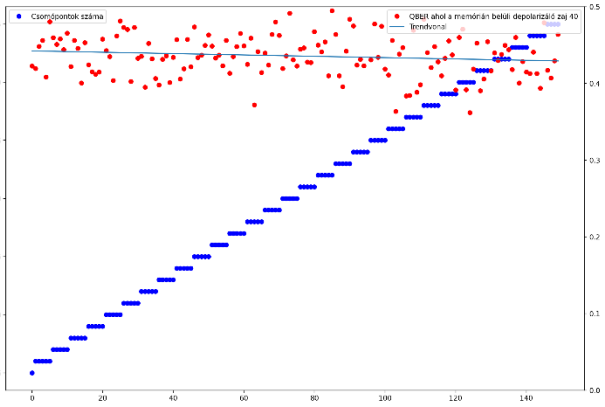
20 Hz



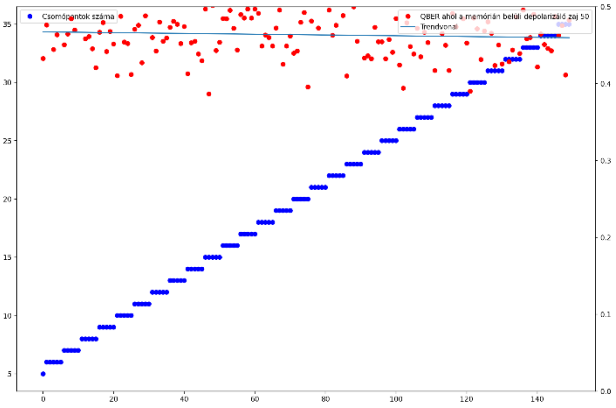
30 Hz



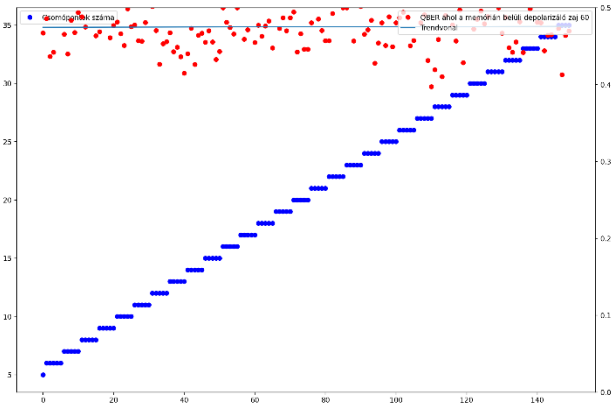
40 Hz



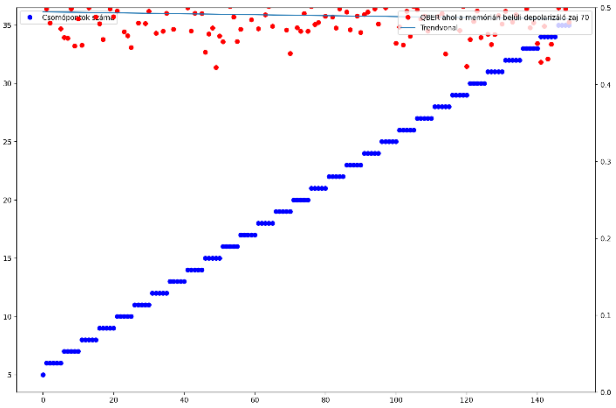
50 Hz



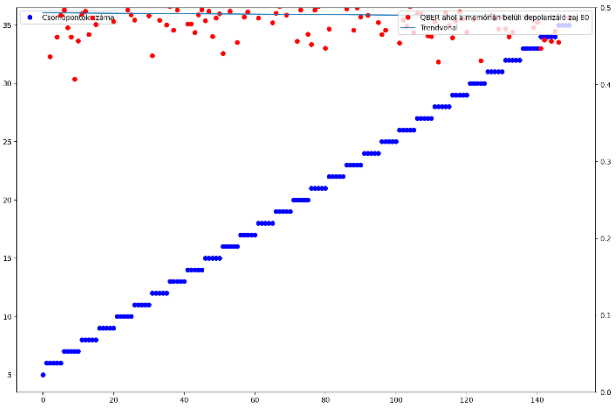
60 Hz



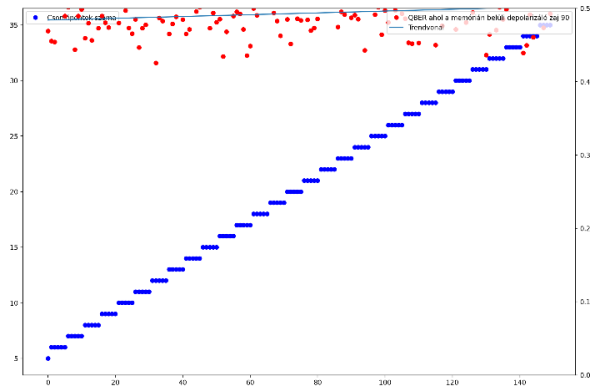
70 Hz



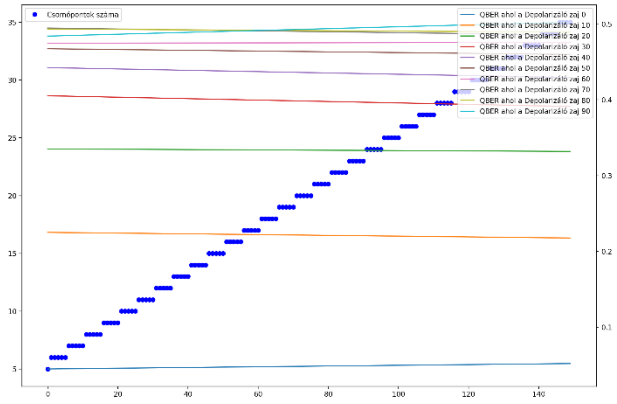
80 Hz



90 Hz



Aggregált



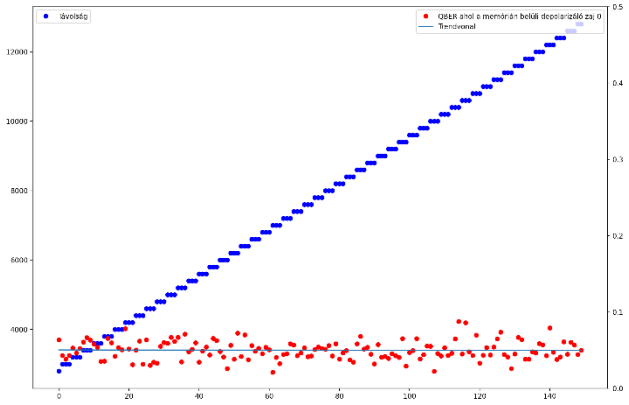
A fenti szimuláció eredményeinek képein megfigyelhetjük, hogy a kvantumbithibaarányra nincs észrevehető hatása a csomópontok számának növelésének. Ennek oka az, hogy míg a csomópontok száma növekedett, a távolság konstans maradt. Emiatt a fotonok által megtett távolság is konstans volt, így a várakozásból eredő kvantumbithibaarány is konstans maradt egy adott depolarizációs rátára.

4.4.3.2 Kulcsszétosztás iteratívan növekvő depolarizációs zajban, időben növekvő útvonal távolságon

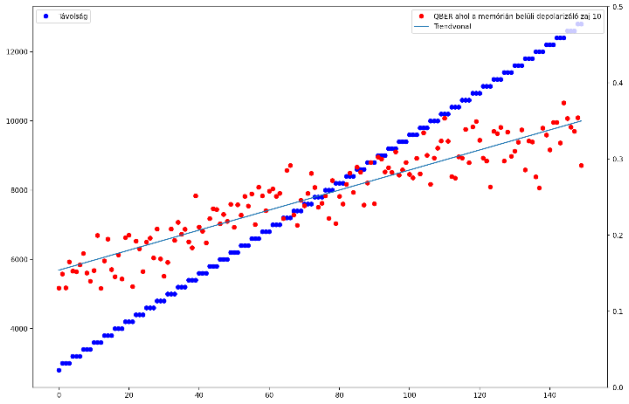
Zavar mértéke [Hz]

Távolság

0 Hz

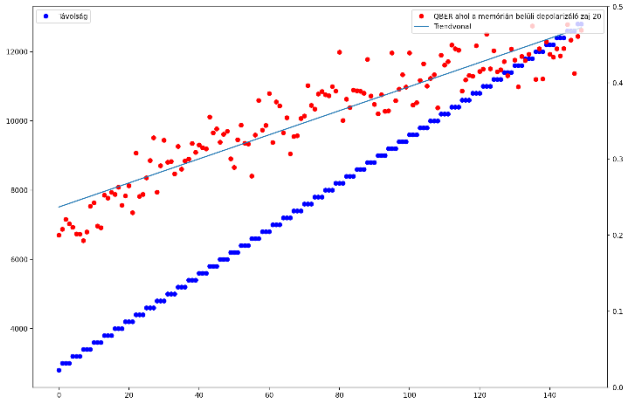


10 Hz

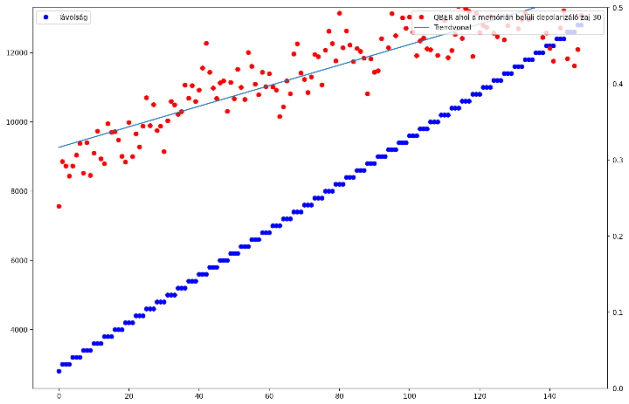


23. ábra: Ebben a szimulációban lehet látni a már eddig többször is említett észrevételt, miszerint a depolarizációs zavar rátából eredő kvantum bithibaarány növekedés összeköttetésben áll a távolsággal. Ennek az oka, hogy a kvantumösszefonódás-csere végrehajtásához, míg a küldött fotonok meg nem érkeznek a célponthoz, a párjukat kvantummemóriában kell tárolni. Emiatt a kvantummemóriában fellépő depolarizáció esélye növekszik a távolsággal.

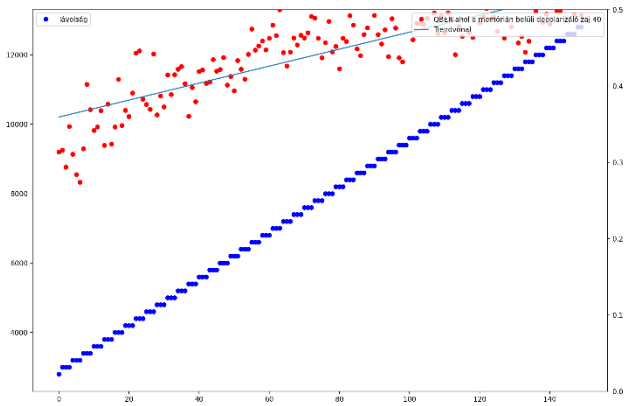
20 Hz



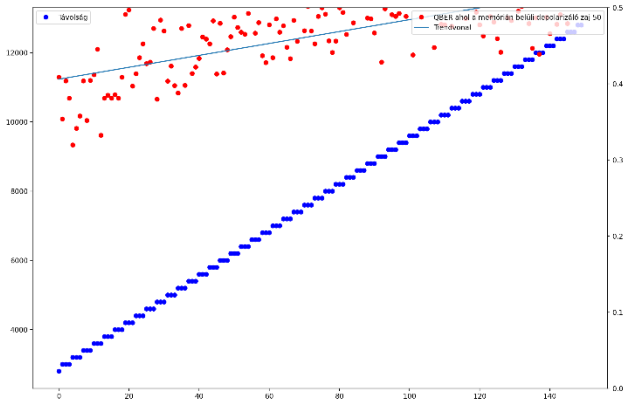
30 Hz



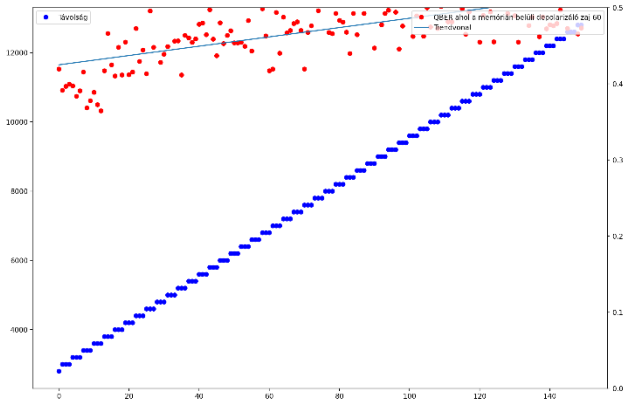
40 Hz



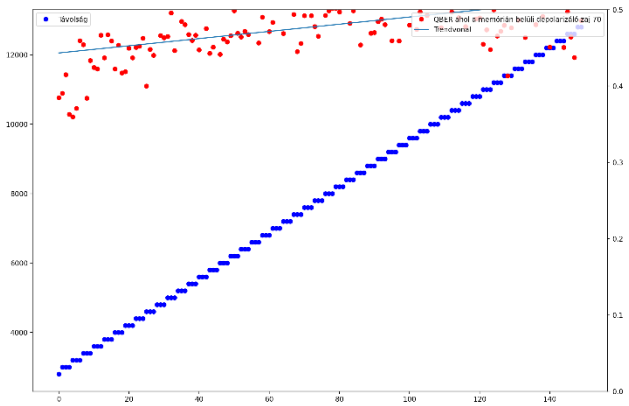
50 Hz



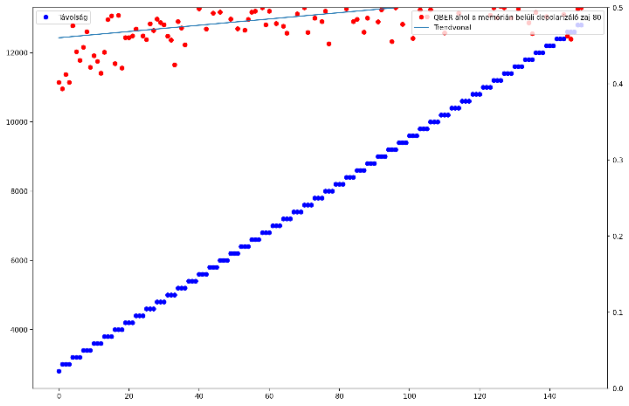
60 Hz



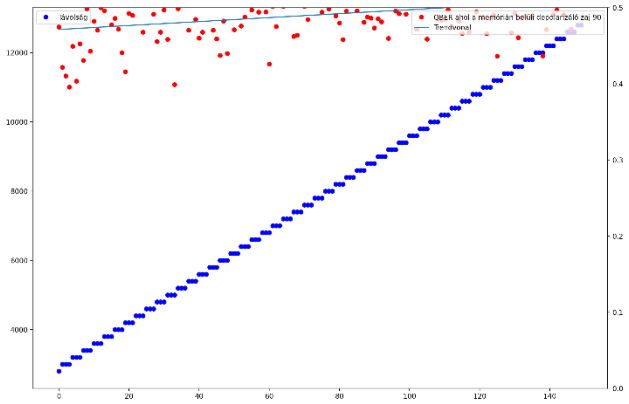
70 Hz



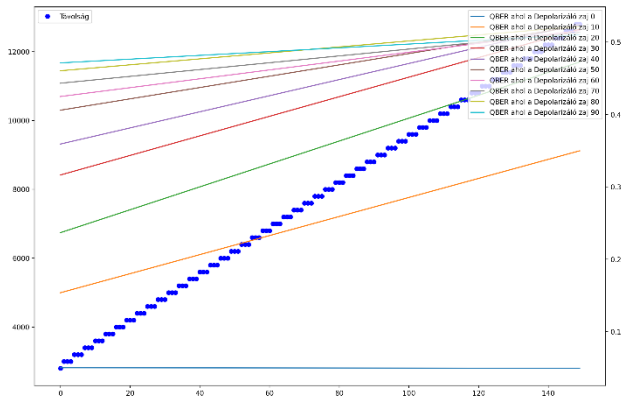
80 Hz



90 Hz



Aggregált



Az fenti szimulációs eredményeken megfigyelhető, hogy a kvantummemória depolarizációs zavarja mellet a kvantumbithiba arányra hatással van a távolságban bekövetkezett változás. Ennek oka a már előző fejezetben is említett tény, miszerint a távolság növekedésével a kvantumbit több időt tölt a kvantummemóriában, emiatt a kvantummemóriában fellépő depolarizációs zajok, nagyobb mértékben befolyásolják.

5 Összefoglalás

Munkám során két kvantumkulcsszétosztó protokoll – BB84 és E91 – műholdas kvantumkommunikációs hálózatban való felhasználásának lehetőségét kutattam. A két protokoll közötti kimagasló különbség az, hogy míg a BB84 protokoll esetén szükséges, hogy a használt csomópontok megbízhatóak legyenek, az E91 esetén ez nem feltétel. A BB84 protokollnak viszont előnye, hogy nincs szükség kvantummemóriára vagy bármi egyéb ma még csak kísérleti stádiumban létező kvantumeszközre.

A BB84 protokoll szimulációja során a kvantum bithibaarány még nagy távolságok esetén is alacsony maradt. Emellett, maga a protokoll által használt elemek mind ma már létező eszközök, ennek köszönhetően egy kezdetleges kvantumhálózat kiépítéséhez tökéletes.

Az E91 protokoll ezzel szemben nem megbízható csomópontokon is megbízható kommunikációt tud folytatni, mivel egy BB84 protokollon futó hálózat esetén, egy csomópont kompromittálását csak újabb biztonsági rendszerek bevonásával tudnák észrevenni. Szerintem egy jövőbeli kvantuminternet esetén sokkal nagyobb élettere lesz az E91 protokollnak, ha sikerül alacsony depolarizációs zavarrátájú kvantummemóriát létrehozni.

A vizsgálataim lehetővé tették, hogy megnézzük, milyen bithibaaránnyal lehet megvalósítani egy közel 600 műholdból álló hálózaton a kulcsok megosztását különböző földi városok között. Egy-egy kommunikáció során nem használtuk fel az összes műholdat, ahogy a csomópontok számait is tartalmazó eredményeim mutatják, elegendő volt általgosan 5 darabot használni.

A szimulációimon keresztül észrevettem, hogy a BB84 protokoll használata esetén a kritikus útvonalrész a föld-űr és az űr-föld mentén található, vagyis egy esetleges útvonal kereső algoritmusnak ezen távolságok minimalizálására kell fokuszáljon leginkább.

Az E91 protokoll alapú rendszerek szimulációs eredményeinek vizsgálata során azt tapasztaltam, az eredeti feltételezésemmel szemben (mint az a két összehasonlító szimulációmban is látható), a távolság az, ami kritikus a kvantumbithibaarány alakulásában. Ez annak köszönhető, hogy a csomópontokon a kvantumösszefonódás-csere időtartama alatt (ami távolságtól függ, hiszen azt be kell járnia a fotonoknak), a kvantumbitet a kvantummemóriában kell tárolni.

Végül, de nem utolsó sorban szeretnék köszönetet nyilvánítani Bacsárdi Lászlónak, aki sokat segített a szimulátor elméleti hátterében, és akit a hét bármely napján bombázhattam kvantumkommunikációval kapcsolatos kérdéseimmel, amelyekre mindig választ is kaptam.

Köszönetnyilvánítás

A kutatás a Kvantumbitek előállítása, megosztása és kvantuminformációs hálózatok fejlesztése nevű, 2017-1.2.1-NKP-2017-00001 számú projekt a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a "Nemzeti kiválósági program" pályázati program finanszírozásában valósult meg.

6 Hivatkozások

[1] E. Technology, „MIT Technology Review,” 2019. [Online]. Available: https://www.technologyreview.com/2019/05/30/65724/how-a-quantum-computer-could-break-2048-bit-rsa-encryption-in-8-hours/. [Hozzáférés dátuma: 17 10 2020].

[2] L. Mgrdichian, „Entanglement Swapping: A New Quantum Trick,” 16 10 2020. [Online]. Available: https://phys.org/news/2007-10-entanglement-swapping-quantum.html. [Hozzáférés dátuma: 16 10 2020].

[3] P. W. S. é. J. Preskill, „Simple Proof of Security of the BB84 Quantum Key Distribution Protocol,” *American Physical Society,* pp. Physical Review Letters 85(2):441-4, 2000.

[4] „SHA-2,” [Online]. Available: https://en.wikipedia.org/wiki/SHA-2. [Hozzáférés dátuma: 16 10 2020].

[5] I. L. C. Michael A. Nielsen, Quantum Computation and Quantum Information 10th anniversary edition, Cambridge University Press, 2010.

[6] D. Lasecki, E91 Quantum Key Distribution Protocol - a step by step proof.

[7] C. Wood, „Trump betting millions to lay the groundwork for quantum internet in the US,” CNBC, [Online]. Available: https://www.cnbc.com/2020/04/27/us-laying-groundwork-for-a-quantum-internet.html. [Hozzáférés dátuma: 17 10 2020].

[8] „Quantum Technologies Flagship,” European Commission, [Online]. Available: https://ec.europa.eu/digital-single-market/en/policies/quantum-technologies-flagship.

[9] „Japan enters quantum computing race -- and offers free test drive,” [Online]. Available: https://asia.nikkei.com/Business/Technology/Japan-enters-quantum-computing-race-and-offers-free-test-drive. [Hozzáférés dátuma: 17 10 2020].

[10] W. K. e. al, „Internet-Draft,” IETF, 12 6 2020. [Online]. Available: https://tools.ietf.org/pdf/draft-irtf-qirg-principles-04.pdf. [Hozzáférés dátuma: 17 10 2020].

[11] „Quantum Repeaters,” Quantum Flagship, [Online]. Available: https://qt.eu/discover-quantum/underlying-principles/quantum-repeaters/. [Hozzáférés dátuma: 17 10 2020].

[12] „NetSquid,” [Online]. Available: https://docs.netsquid.org/latest-release/learn_examples/learn.examples.repeater_chain.html. [Hozzáférés dátuma: 16 10 2020].

[13] „N2YO,” [Online]. Available: https://www.n2yo.com/api/. [Hozzáférés dátuma: 16 10 2020].

[14] L. Bacsardi, Efficient Quantum Based Space Communications, LAP Lambert Academic Publishing , 2013.

[15] „A. Kiss, M. Galambos, L. Bacsárdi, Refined computer simulation of loss,” *InProc. of 69th International,* p. 8, 2018.

[16] „M. Suchara et al "QuRE: The Quantum Resource Estimator toolbox," 2013 IEEE 31st International Conference on Computer Design (ICCD), Asheville, NC, 2013, pp. 419-426, doi: 10.1109/ICCD.2013.6657074.”.

[17] S. Imre és F. Balázs, Quantum Computing and Communications An Engineering Approach, Budapest: John Wiley & Sons Ltd, 2005.

[18] V. F. M. N. D. Alberto Carrasco-Casado, „ReasearcGate,” [Online]. Available: https://www.researchgate.net/figure/BB84-protocol-basic-scheme_fig11_309731586. [Hozzáférés dátuma: 17 10 2020].